Lehrstuhl für Kommunikationsnetze
Prof. Dr.-Ing. Christian Wietfeld

Entwurf und Leistungsbewertung von Ad-hoc-Kommunikationsnetzen für den Katastrophenschutz

Genehmigte Dissertation
zur Erlangung des akademischen Grades eines
Doktors der Ingenieurwissenschaften (Dr.-Ing.)
der Fakultät für Elektrotechnik und Informationstechnik
der Technischen Universität Dortmund

von
Dipl.-Ing. Andreas Herbert Wolff
aus
Düsseldorf

Hauptreferent:	Prof. Dr.-Ing. Christian Wietfeld
Korreferent:	Prof. Dr.-Ing. Rüdiger Kays
Dissertation eingereicht am:	25.06.2013
Tag der mündlichen Prüfung:	23.09.2013

Für meine Kinder
Leon und Maximilian

Danksagung

Diese Doktorarbeit ist während meiner Tätigkeit am Lehrstuhl für Kommunikationsnetze der TU Dortmund entstanden. Mein aufrichtiger Dank gilt meinem Doktorvater Prof. Dr.-Ing. Christian Wietfeld, für seine Motivation, inspirierende Ratschläge und hilfreiche Unterstützung.

Für die Übernahme des Korreferats und die intensive Auseinandersetzung mit meiner Doktorarbeit danke ich Prof. Dr.-Ing. Rüdiger Kays. Darüber hinaus bedanke ich mich bei den weiteren Mitgliedern der Prüfungskommission Herrn Prof. Dr.-Ing. Stephan Frei und Herrn Prof. Dr.-Ing. Christian Rehtanz.

Außerdem danke ich dem Bundesministerium für Bildung und Forschung (BMBF) für die Finanzierung dieser Arbeit im Rahmen des Forschungsprojektes SPIDER. In diesem Zusammenhang möchte ich meinen Dank allen Projektpartnern für die erfolgreiche Zusammenarbeit zum Ausdruck bringen. Insbesondere bedanke ich mich bei Brandrat Ansgar Stening von der Feuerwehr Gelsenkirchen für die inspirierende Zusammenarbeit.

Besonderer Dank geht an Mohamad Sbeiti und Sebastian Subik für wertvolle und anregende Diskussionen. Herzlichen Dank an alle Studenten und wissenschaftlichen Hilfskräfte, die zu meiner Forschung während ihrer Zeit am CNI beigetragen haben.

Für das inhaltliche Lektorat bedanke ich mich bei Mohamad Sbeiti, Markus Putzke, Christoph Ide und Carsten Rietfort. Ferner bedanke ich mich bei meinem Vater Dr. Gunter E. Wolff für die Korrektur der Arbeit.

Außerdem geht mein besonderer Dank an meine Familie, für ihre emotionale Unterstützung und den Rückhalt, den ich in schweren Situationen gebraucht habe.

Schließlich danke ich meiner wundervollen Frau Christina für ihre Liebe, ihre tatkräftige Unterstützung und unerschöpfliche Geduld.

Andreas Herbert Wolff *Essen, September 2013*

Kurzfassung

Ein zuverlässiges Kommunikationsnetz stellt die wesentliche Basis für zukünftige, IT-gestützte Dienste für Rettungskräfte an einem Schadensort dar. Heutzutage basiert die Kommunikation im Katastrophenschutz auf dem digitalen Behördenfunk TETRA, bzw. in Teilen noch auf dem analogen BOS-Funk. Diese bieten keine ausreichende Datenrate für Multimedia-Anwendungen. Existierende Infrastrukturnetze, wie z.B. das öffentliche Mobilfunknetz, können bei einer Großschadenslage überlastet sein oder beschädigt werden und sind daher für Rettungskräfte nicht uneingeschränkt nutzbar. Um neue Multimedia Dienste am Schadensort zuverlässig nutzen zu können, sind Rettungskräfte daher auf ihr eigenes lokales Kommunikationsnetz angewiesen. Für die Rettungskräfte ist ein praktikabler Netzaufbau essentiell, wobei die Technik den Einsatzablauf nicht behindern darf. Zudem bestehen Anforderungen an die Dienstgüte des Netzes und die Leistungsfähigkeit in Bezug auf die Datenrate, da z.B. Videos von Helmkameras übertragen werden sollen.

Ziel dieser Arbeit ist der Entwurf und die Leistungsbewertung von praxistauglichen Kommunikationslösungen für Ad-hoc-Netze im Katastrophenschutz. Zur Realisierung eines benutzerfreundlichen Netzaufbaus wird ein praxistaugliches Vernetzungskonzept vorgestellt, welches einen selbstkonfigurierenden Ad-hoc-Aufbau erlaubt. In enger Zusammenarbeit mit der Feuerwehr werden rettungsprozesskonforme Netz-Aufbaustrategien erforscht, welche die Rettungskräfte bei ihrer Arbeit nicht einschränken und als Basis für eine zuverlässige Kommunikation genutzt werden können.

Die wesentliche Basistechnologie des Lösungsansatzes ist 802.11-basierte Kommunikation, welche im 5 GHz Band betrieben wird. WLAN Stationen eines Netzes können sich gegenseitig stören oder durch andere Netze gestört werden. In dieser Arbeit wird daher ein neuartiges Verfahren zur Verringerung der Interferenz vorgestellt. Der im Rahmen der Arbeit entwickelte *Interference Avoidance Algorithm* (IAA) deaktiviert redundante Router im Netz der Rettungskräfte. Mittels Simulation wurde gezeigt, dass in den untersuchten Szenarien im Durchschnitt eine höhere *packet delivery ratio* im Vergleich zur Vernetzung ohne IAA erreicht wird.

Um Störungen, die durch andere Netze verursacht werden, zu verringern, wird im Rahmen der Arbeit eine Priorisierung der Kommunikation der Rettungskräfte durch die Einführung von neuen Kommunikationsklassen vorgeschlagen. Dieses Konzept basiert auf der Modifikation der Parameter der verteilten Medienzugriffsfunktion (DCF) von WLAN, ähnlich dem IEEE 802.11e jedoch noch höher priorisiert, und wird *Emergency-DCF* genannt. Für deren Leistungsbewertung wurde ein existierendes analytisches Markov-Modell modifiziert und erweitert. Anschließend werden die analytischen Ergebnisse simulativ validiert. Die Machbarkeit des Verfahrens wird weiterhin im Experiment validiert.

Die in der Arbeit vorgestellten Forschungsergebnisse sind in Verbundprojekte eingeflossen, in denen neben Industriepartnern auch Anwender aktiv beteiligt waren. So konnte das entwickelte Vernetzungskonzept im Projekt MobileEmerGIS zusammen mit der Feuerwehr Dortmund erprobt werden. Darüber hinaus ist die prozesskonforme Vernetzung im BMBF Projekt SPIDER durch die Feuerwehr Gelsenkirchen in Feldtests validiert worden. Das Vernetzungskonzept wurde in einer modifizierten Version ebenfalls für die Vernetzung der Flugroboter im BMBF Projekt *Airshield* eingesetzt.

Durch mehrere Veröffentlichungen auf Konferenzen und Präsentationen auf Workshops konnte eine internationale Resonanz erzielt werden. Die im Rahmen der Arbeit entwickelten Verfahren werden aktuell in Kooperation mit dem DRK in Bayern im Einsatz erprobt.

Abstract

A reliable communications network provides the essential basis for future IT-based services for rescue personnel at an incident scene. Nowadays, the communication in civil protection is based on the digital trunked radio TETRA system, or is still based on analog BOS radio system. These systems do not provide sufficient data rate for multimedia applications. Existing infrastructure networks, such as the public mobile telephony network, can be damaged in a major incident situation and therefore are not fully usable for rescue personnel. To use new multimedia services at the incident scene, rescue personnel therefore dependent on their own local communications network. For the rescue personnel a practicable network deployment is essential, whereas the technology should not hinder the rescue process. Moreover, there are demands on the quality of service of the network, and the performance in terms of the data rate, as for example videos should be transferred from helmet cameras.

The aim of this thesis is the design and performance evaluation of a robust communications solution for ad hoc networks in disaster management. To enable a user-friendly network deployment, a reliable networking approach is presented which allows a self-configuring ad hoc deployment. Working closely with the fire department, rescue process-compliant network deployment strategies are investigated which can be used as a basis for reliable communication.

The key enabling technology of the approach is Wi-Fi communication, which operates in 5 GHz band. WLAN stations of one network can interfere with each other or can be interfered by other networks on the same channel. In this work, a method for reducing the interference is introduced. The proposed Interference Avoidance Algorithm (IAA) disables redundant router in the network of rescue personnel. It can be shown by simulations that on average in the investigated scenarios a higher packet delivery ratio can be achieved when IAA is active compared to networks without IAA.

In order to reduce interference caused by other networks, a prioritization of the communication of the rescue personnel with the introduction of new communication classes is proposed. This concept is based on the modification of the parameters of the medium access function (DCF) of wireless LAN, which is comparable with IEEE 802.11e but is more prioritized, and is called Emergency-DCF. For its performance evaluation, an existing Markov model is modified and extended. Then, the analytical results are validated by simulation. The feasibility of the method can be validated experimentally.

The presented solutions of this thesis have been developed within and were contributed to research projects, where partners from the industry and end-users were actively involved. Thus, the network concept developed within this thesis was tested together with the Dortmund fire brigades during the project MobileEmerGIS. Moreover, the process oriented networking was validated during field tests by Gelsenkirchen fire brigade during the BMBF project SPIDER. The networking concept was also used in a modified version for networking the flying robots in the BMBF project Airshield.

With several publications in conferences and presentations at workshops, an international resonance has been achieved. Currently, the results of this thesis are being deployed with the German Red Cross in Bavaria.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AC	Zugriffskategorie
AIFS	Arbitration Interframe Space
AIFSN	Arbitration Interframe Space Number
AODV	Ad-hoc On-Demand Distance Vector
AP	Access Point
APCO	Association of Public Safety Communications Officials
ARM	Advanced RISC Machines
BATMAN	Better Approach To Mobile Ad-hoc Networking
BMBF	Bundesministerium für Bildung und Forschung
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BSS	Basic Service Set
BTS	Base Transceiver Station
CAP	Controlled Access Phase
CDMA	Code Division Multiple Access
CFP	Contention Free Period
CMS	Core Management Service
CNI	Communication Networks Institute
CP	Contention Period
CPU	Central Processing Unit
CTS	Clear To Send
CW	Contention Window
DCF	Distributed Coordination Function
DIFS	DCF Interframe Spaces
DPN	Disconnected Polymorphous Network
EDCA	Enhanced Distributed Channel Access
EDCF	Emergency-DCF
EIRP	Equivalent Isotropically Radiated Power - Äquivalente isotrope Sendeleistung
FuG	Funkgerät, gebaut aufgrund eines Pflichtenheftes einer Behörde
GIS	Geographisches Informationssystem
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function

HiMoNN	Highly Mobile Network Node
HSPA	High Speed Packet Access
HWMP	Hybrid Wireless Mesh Protokoll
IEEE	Institute of Electrical and Electronics Engineers
IFS	Inter Frame Space
IP	Internet Protocol
KIT	Krisenintervention im Rettungsdienst
MORE	Network-centric Middleware for Group communication and Resource Sharing across Heterogeneous Embedded Systems
MUAV	Micro Unmanned Aerial Vehicle
NAV	Network Allocation Vector
OGM	Originator Message
OLSR	Optimized Link State Routing
PAN	Personal-Area-Network
PC	Personal Computer
PCF	Point Coordination Function
PIFS	PCF Interframe Space
PRML	Protection and Rescue Markup Language
QAP	QoS Access Point
QBSS	QoS Basic Service Set
QoS	Quality of Service - Dienstgüte
QSTA	QoS supporting Stations
RISC	Reduced Instruction Set Computer - Rechner mit reduziertem Befehlssatz
RS232	Recommended Standard 232 - Serielle Schnittstelle
RTS	Request To Send
SF_{DUR}	Dauer eines Superframes
SIFS	Short Interframe Space
SOA	Service-Oriented-Architecture
SOAP	Simple Object Access Protocol
SPIDER	Security System for Public Institutions in Disastrous Emergency scenaRios
STA	IEEE 802.11 Station
TBTT	Target Beacon Transmission Time

TETRA	Terrestrial Trunked Radio
TTL	Time-To-Live
TXOP	Transmission Opportunity
UART	Universal Asynchronous Receiver Transmitter
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
UWB	Ultra-Breitband-Technologie
VPN	Virtual Private Network
WAN	Wide-Area-Network
WiFi	Synonym für WLAN
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPA2	WiFi Protected Access 2
XML	Extensible Markup Language
XML-IF	XML-Schnittstelle

Symbolverzeichnis

AC_A	Zugriffskategorie A
AC_B	Zugriffskategorie B
$b_{A(r,k)}$	Zustandswahrscheinlichkeit für den Zustand (r,k) in dem zweidimensionalen Markov-Ketten Modell in Abbildung 5.7 für AC_A
$b_{B(r,k)}$	Zustandswahrscheinlichkeit für den Zustand (r,k) in dem zweidimensionalen Markov-Ketten Modell in Abbildung 5.9 für AC_B
CW	Wettbewerbsfenster (engl. *Contention Window*) der IEEE 802.11 Backoff Prozedur für den zufallsbasierten Kanalzugriff
CW_{maxA}	Maximalgröße des Wettbewerbsfensters für AC_A
CW_{maxB}	Maximalgröße des Wettbewerbsfensters für AC_B
Δ_{DIFS}	Unterschied zwischen $DIFS_A$ und $DIFS_B$
$DIFS_A$	Dauer eines DIFS für die AC_A
$DIFS_B$	Dauer eines DIFS für die AC_B
$d(k)$	Zustandswahrscheinlichkeit für den Zustand (k) in dem eindimensionalen Markov-Ketten Modell in Abbildung 5.11.
$E[A]$	Durchschnittlicher effektiver Payload für AC_A
$E[B]$	Durchschnittlicher effektiver Payload für AC_B
$E[P]$	Effektiver Payload in einem Datenframe
EZ	die mittlere Zeitdauer zwischen zwei aufeinander folgenden Übertragungen
P_{bA}	Wahrscheinlichkeit, dass eine AC_A Station einen belegten Kanal sieht, direkt nachdem die Station einen IFS[A], seit dem Ende der letzten Kanalbelegung, gewartet hat
P_{bB}	Wahrscheinlichkeit, dass eine AC_B Station einen belegten Kanal sieht, direkt nachdem die Station einen IFS[B], seit dem Ende der letzten Kanalbelegung, gewartet hat
P_{col}	Wahrscheinlichkeit, dass eine Kollision in einem *time slot* auftritt
P_{idle}	Wahrscheinlichkeit, dass für eine Station ein *idle time slot* auftritt
P_{idleA}	Durchschnittliche Wahrscheinlichkeit, dass sich eine AC_A Station in einem *idle time slot* befindet
P_{idleB}	Durchschnittliche Wahrscheinlichkeit, dass sich eine AC_B Station in einem *idle time slot* befindet
$Pr_{A(r)}$	Wahrscheinlichkeit, dass eine AC_A Station eine Backoff Prozedur mit einem Startwert r beginnt
$Pr_{B(r)}$	Wahrscheinlichkeit, dass eine AC_B Station eine Backoff Prozedur mit einem Startwert r beginnt
$Pr(r)$	Wahrscheinlichkeit, dass eine Station eine neue Backoff Prozedur mit einem Startzählwert r beginnt
P_{sB}	Wahrscheinlichkeit, dass eine AC_B Station einen belegten Kanal sieht, innerhalb des IFS[B] Zeitraums, seit dem Ende der letzten Kanalbelegung

S_A	Sättigungsdurchsatz für jede AC_A Station
S_B	Sättigungsdurchsatz für jede AC_B Station
τ_A	Sendewahrscheinlichkeit einer AC_A Station
τ_B	Sendewahrscheinlichkeit einer AC_B Station
T_c	Verbrauchte Zeit bei einer Kollision
$timeslot$	Dauer eines IEEE 802.11 Zeitschlitzes
T_s	Benötigte Zeit für eine erfolgreiche Übertragung

1 Einleitung

Im Katastrophenschutz findet derzeit eine Evolution der verwendeten Kommunikationsnetze statt. Der analoge BOS-Funk wird durch den digitalen Behördenfunk TETRA ersetzt. Dabei bleibt die Sprachkommunikation die Hauptanwendung. Im Rahmen von Forschungsprojekten äußern Rettungsorganisationen, allen voran die Feuerwehren, die Anforderung, neben Sprache auch Videos, Fotos und Sensorwerte zu übertragen [88]. Dabei benötigt vor allem die Übertragung von Videos hohe Datenraten.

In [63] stellt *Pinson* Untersuchungsergebnisse vor, welche die minimale Auflösung und Framerate für Videoanwendungen im Katastrophenschutz angibt, die von den Endanwendern noch akzeptiert werden. Dabei wird eine minimale Datenrate von 768 kbit/s für ein Video mit einer Auflösung von 720 x 486 Bildpunkten benötigt, welches mit H.264 codiert wurde. Die erforderliche Datenrate für diese Anwendungen stellt der digitale Behördenfunk TETRA nicht zur Verfügung.

Das TETRA-Netz ist vergleichbar mit dem Mobilfunknetz der zweiten Generation (GSM) [92]. Bei TETRA wird beispielsweise auch ein Zeitmultiplexverfahren ähnlich wie bei GSM eingesetzt, wobei aber bei TETRA jede Frequenz nur in vier anstatt acht Zeitschlitze aufgeteilt wird. Die Entwicklung des mobilen Internets hat gezeigt, dass erst mit einer hohen Datenrate multimediale Dienste realisiert werden können. Eine GSM ähnliche Verbindung mit nur vier Zeitschlitzen (max. 37,6 kbit/s) bietet keine hinreichende Datenrate (siehe TETRA-Spezifikation [20]). Derzeit ist der Hauptanwendungsfall von TETRA die digitale Sprachübertragung.

Eine alternative Nutzung von TETRA ist die Übertragung von Fahrgastinformationen im öffentlichen Nahverkehr. So werden in Dortmund die Anzeiger an Haltestellen, welche die aktuelle Verspätung der Busse und Bahnen anzeigen, per TETRA gespeist [76]. Dazu wird der *Short Data Service*, kurz SDS, eingesetzt, der vergleichbar zum *Short Message Service*, kurz SMS, im GSM-Mobilfunknetz ist.

Da das eigentliche Kommunikationsnetz der Rettungskräfte nicht die erforderliche Datenrate für die neuen Multimedia-Dienste liefert, müssen die Daten der Anwendungen über ein zusätzliches Kommunikationsnetz übertragen werden. Die

Abbildung 1.1: Anforderungen an Krisenkommunikationstechnik [94]

qualitativen Anforderungen an ein solches Netz sind in Abbildung 1.1 zusammengefasst. Die im Rahmen dieser Arbeit behandelten Anforderungen sind:

- Ad-hoc Netzaufbau,
- Lückenlose Abdeckung; auch in Kellern, Tunnels, Tiefgaragen und Wäldern,
- Bedienbarkeit unter Einsatzbedingungen,
- QoS Unterstützung,
- Austausch von Multimediadaten (z.B. Bilder, Karten und Videos).

Ein denkbares Zusatznetz, auf welches die Rettungskräfte am Einsatzort zugreifen könnten, wäre das öffentliche Mobilfunknetz. Dieses ist jedoch im Krisenfall nicht zuverlässig, wie die Erfahrung mit der Krisenbewältigung bei der Loveparade in Duisburg 2010 gezeigt hat [65]. Dabei ist die Kommunikation der Polizei über die Mobilfunknetze laut Polizeibericht aufgrund von „temporären Überlastungen der jeweiligen Mobilfunknetze (hohe Anzahl gleichzeitig geführter Gespräche)“ [65] zusammengebrochen. Zwar sind im Mobilfunknetz Vorrangschaltungen möglich, um die Kommunikation der Rettungskräfte zu priorisieren, aber diese müssen zuvor beantragt werden und stehen nicht permanent zur Verfügung [74]. Im Falle einer plötzlich auftretenden Großschadenslage können Rettungsorganisationen daher nicht sicher auf die öffentlichen Mobilfunknetze zugreifen.

1.1 Ad-hoc-Netze für den Katastrophenschutz

Wenn nun auf das öffentliche Mobilfunknetz aufgrund von möglichen Ausfällen oder Engpässen nicht zurückgegriffen werden kann, und der digitale Behördenfunk nicht ausreichend für neuartige Multimedia-Dienste dimensioniert wurde, dann bleiben nur die Alternativen, ein zusätzliches Netz vor Ort aufzubauen, oder ein vorhandenes Vor-Ort-Netz für die eigenen Zwecke zu nutzen. Viele Großschadenslagen finden jedoch an Orten statt, wo möglicherweise keine lokalen Netze vorhanden sind. Darüber hinaus können vor Ort vorhandene lokale Netze aufgrund der Großschadenslage fehlerhaft und unzuverlässig werden. Daher ist die sicherste Alternative ein eigenes lokales Kommunikationsnetz, bei welchem die volle Kontrolle über das Netz gewährleistet ist.

Für die Wahl der zugrunde liegenden Technologie stehen mehrere Alternativen zur Verfügung, die unterschiedliche Reichweiten und Datenraten anbieten (siehe Abbildung 1.2). Beispielsweise könnten mit Hilfe von Pico-, oder Femtozellen eigene UMTS-Netze aufgebaut werden. Dies hätte den Vorteil, dass die meisten Rettungskräfte über private UMTS-fähige Endgeräte verfügen und somit die Informationen schnell verteilt werden können. Dazu ist jedoch eine Breitbandverbindung an das Internet vorgesehen, damit das Core-Netz des Mobilfunknetzes erreicht werden kann [77]. Diese Internetverbindung steht jedoch möglicherweise am Einsatzort nicht zur Verfügung.

Eine weitere Alternative ist der Einsatz von WiMAX als lokale Vernetzungstechnologie [38]. WiMAX liefert die erforderliche Datenrate und kann auch mit einer großen Anzahl von Nutzern effizient umgehen, da es über ein zentrales Zugriffsverfahren verfügt [108]. Dabei steuert die WiMAX-Basisstation den Kanalzugriff und kann anhand von Priorisierungen festlegen, welcher Nutzer wie viel Datenrate zur Verfügung hat. Der große Nachteil von WiMAX ist jedoch, dass es kaum Endgeräte gibt, die WiMAX unterstützen. Große Hersteller wie Intel haben immer wieder angekündigt, WiMAX in die kommende Generation ihrer Chipsätze zu integrieren, jedoch ist bisher noch nichts in dieser Richtung geschehen.

Der Einsatz des weit verbreiteten Standards IEEE 802.11 [40] (in Abbildung 1.2 grau markiert) für die Vernetzung der Rettungskräfte setzt voraus, dass die drahtlose Kommunikationstechnologie für diesen Zweck tauglich ist. Dies wurde von *Hofmann et al.* in [31] für Szenarien, in denen Feuer, Rauch und Wasserdampf auftreten, untersucht. Es stellte sich heraus, dass Feuer und Rauch kaum Auswirkungen auf die Kommunikationsqualität haben. Wasserdampf hingegen erhöht den Jitter um ca. 100 ms und verringert die Kommunikationsreichweite um ca. 20%. Beide Effekte können jedoch kompensiert werden und stellen keine erhebliche Einschränkung dar [31]. Daher wird in dieser Arbeit IEEE 802.11, das mithin noch das beste Profil aufweist, als Kommunikationstechnologie eingesetzt.

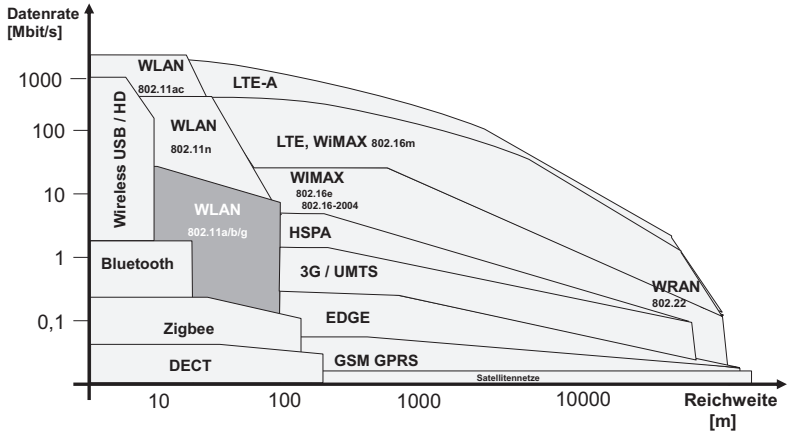


Abbildung 1.2: Kommerzielle Mobilfunktechnologien im Überblick [95]

In Deutschland ist IEEE 802.11 unter der Abkürzung WLAN, *Wireless Local Area Network*, bekannt. Im angelsächsischen Raum wird eher die Bezeichnung WiFi verwendet. Die WLAN-Technologie und deren Umsetzung in Hardware erfüllt die Anforderungen der Rettungskräfte. Diese brauchen Hardware, welche günstig ist, sich einfach bedienen lässt und Dienste unterstützt, die von den Rettungskräften eingesetzt werden. Zu diesen Diensten zählt unter anderem die drahtlose Übertragung von Videos und von digitalen Lagebildern. Der im Rahmen dieser Arbeit eingesetzte WLAN-Standard nach IEEE 802.11a erreicht eine Bruttodatenrate von 54 Mbit/s und bietet damit eine in der Regel ausreichende Datenrate für die Realisierung dieser Dienste. Darüber hinaus ist WLAN-Hardware günstig und kann auch infrastrukturlos im Ad-hoc-Modus betrieben werden. Mittels vorkonfigurierter Hardware sind WLAN Ad-hoc-Netze benutzerfreundlich einsetzbar.

Eine weitere Anforderung der Rettungskräfte an das Kommunikationsnetz ist die nahezu komplette Funkabdeckung eines Einsatzortes. Aufgrund der regulatorischen Begrenzung der EIRP (äquivalente isotrope Strahlungsleistung) von WLAN-Hardware auf 100 mW ergibt sich bei 2,4 GHz in der Regel eine Reichweite von ca. 10 m bis 80 m in Gebäuden. Für den Außenbereich wird häufig eine nominelle Reichweite von 250 m angenommen, die auch bei vielen Untersuchungen in diesem Bereich angenommen wird (siehe z.B. [58], [106] und [90]). Die Sendeleistungsbeschränkung basiert auf der internationalen Funkdienstordnung der ITU [43]. Insbesondere in Gebäuden ist diese Reichweite aufgrund der Dämpfung von Mauern und anderen Gegenständen stark reduziert [83]. Die Ausdehnung eines Einsatzortes ist meist größer als 250 m und reicht häufig auch in Gebäude hinein. Die Anforderung der Funkabdeckung kann hierbei durch die Multi-Hop-Kommunikation mittels eins WLAN Mesh-Netzes erfüllt werden. Hierzu werden Routing-Protokolle eingesetzt,

die einen Kommunikationspfad über mehrere Knoten hinweg zu einem Empfänger auffinden [8]. Insbesondere werden hierfür die beiden Protokolle OLSR [12] und BATMAN [44] eingesetzt, welche in der berliner Freifunk-Community zum Einsatz kommen und damit ihre Praxistauglichkeit unter Beweis gestellt haben [54]. Einige Eigenschaften der drahtlosen Ad-hoc-Kommunikation sind in [62] zusammengefasst.

Yarali et al. stellen in [105] mobile Mesh-Netze als Schlüsseltechnologie für die Bewältigung von Großschadenslagen vor. Ein umfassender Lösungsansatz für die IT-gestützte Krisenbewältigung wird von *Fragkiadakis et al.* in [22] dargestellt. Sie führen eine flexible Netzarchitektur ein, welche eine gemeinsame Austauschplattform für heterogene Multi-Operator-Netze bei Großschadenslagen bereitstellt. Dabei stellen mobile Mesh-Netze die Basistechnologie dar.

Im Rahmen des vom BMBF geförderten Projekts SPIDER [85] wurde eine Anforderungsanalyse bezüglich des Kommunikationsnetzes durchgeführt. Hierbei wurde in Gesprächen mit der Feuerwehr festgestellt, dass ein mobiles Mesh-Netz eine geeignete Lösung zur Vernetzung der Rettungskräfte vor Ort ist. Es können tragbare *Mesh Router*, die sehr leicht sind, für den Netzaufbau eingesetzt werden (vgl. *Dropped Units* in [100]). Ähnliche Geräte setzen *Souryal et al.* [79] für ihre Untersuchungen ein. Die Feuerwehr hat aber betont, dass die *Mesh Router* nicht den Rettungsprozess beeinträchtigen dürfen, sondern eher in den Rettungsprozess integriert werden sollen. Zu diesem Zweck wurde von *Liu et al.* [50] ein automatischer *Relay*-Spender, der am Gürtel getragen wird, vorgeschlagen (siehe Kapitel 2.1.4). Dieser ist zwar für den Aufbau des Netzes sinnvoll, aber die Rettungskräfte müssen beim Einsatzende die *Relays* einzeln vom Boden auflesen. Daher wird hier eine neuartige Lösung vorgeschlagen, bei der die *Relays* sowohl während des Rettungsprozesses ausgebracht werden, als auch nach Einsatzende *on-the-fly*, also im Zuge ihrer gewöhnlichen Handlungen, eingesammelt werden. Möglich wird dies durch die Integration der *Mesh Router* in Ausrüstungsgegenstände der Einsatzkräfte, beispielsweise in die Kupplungen der Feuerwehrschläuche.

IEEE 802.11 erfüllt somit die grundsätzlichen Anforderungen der Rettungskräfte an das Kommunikationsnetz und wird daher im Rahmen dieser Arbeit als Technologie für den Betrieb eines Kommunikationsnetzes für Rettungskräfte am Einsatzort ausgewählt.

1.2 Vernetzungskonzept für Rettungskräfte

Im Falle einer Großschadenslage wird sich der Einsatzleiter samt Führungsstab im Freifeld in sicherer Entfernung zum Schadensereignis aufhalten. Die Einsatzkräfte selbst müssen auch ein betroffenes Gebäude betreten. Dabei sollte die WLAN-Verbindung nicht unterbrochen werden, damit sich der Einsatzleiter z.B. zu jeder

Zeit über die Helmkamera der Einsatzkräfte, auch innerhalb der Gebäude, ein Bild der vorherrschenden Lage machen kann.

Um eine WLAN-Verbindung über größere Entfernung und auch in Gebäude hinein aufrecht zu erhalten, existieren verschiedene Lösungsansätze. Ein denkbarer Ansatz könnte beispielsweise sein, die Endgeräte der einzelnen Rettungskräfte als *Router* einzusetzen. Hierbei sind jedoch Situationen denkbar, bei denen viel Verkehr über ein einzelnes Endgerät geleitet wird, welches aufgrund der Mobilität der Teilnehmer auch die Verbindung zum Rest des Netzes verlieren kann. Verliert dieser Teilnehmer jedoch den Kontakt zum Gateway im Netz, so wird auch der Kontakt zu den anderen Teilnehmern, die ihren Verkehr über diesen Teilnehmer geleitet haben, unterbrochen. Die Anforderung an ein zuverlässiges Kommunikationsnetz kann daher von den rein mobilen Ad-hoc-Netzen nicht erfüllt werden.

In dieser Arbeit wird daher zunächst das so genannte *Dropped Units* Konzept vorgestellt. Dabei wird mit Hilfe von batteriebetriebenen WLAN-Routern ein quasi stationäres lokales Netz aufgebaut. Sobald der Empfang schlecht wird, bauen die Rettungskräfte vom Einsatzleitwagen ausgehend ein Kommunikationsnetz auf, indem sie *Dropped Units* platzieren. Dieses stationäre Netz bietet den Rettungskräften nach seinem Aufbau ein zuverlässiges Kommunikationsnetz.

Da das Ad-hoc-Netz der Einsatzkräfte auch an Orten aufgebaut werden kann, an denen bereits eine WLAN-Infrastruktur besteht, stellt sich die Frage, inwieweit sich das Ad-hoc-Netz und die bestehenden Netze gegenseitig stören. Der WLAN-Standard erlaubt beispielsweise im 2,4 GHz Band einen gleichzeitigen, störungsfreien Betrieb von drei unabhängigen Übertragungen [40]. Falls am Einsatzort noch funktionsfähige WLAN-Netze existieren, muss im *worst case* davon ausgegangen werden, dass alle Kanäle am Einsatzort belegt sind. Ausgehend von der IEEE 802.11e Standardisierung für WLAN [37], welche die Unterstützung von Dienstgüte bei der drahtlosen Übertragung ermöglicht, wird im Rahmen dieser Arbeit ein neuartiges Priorisierungsverfahren, Emergency-DCF genannt, vorgestellt, um die Störungen der vorhandenen WLAN-Netze auf das Ad-hoc-Netz der Einsatzkräfte möglichst gering zu halten. Da an einem Einsatzort schon ein Netz vorhanden sein könnte, welches 802.11e verwendet, sind die Zugriffskategorien der Emergency-DCF höher priorisiert, als die Kategorien von 802.11e. Darüber hinaus unterstützten zu Beginn der vorliegenden Arbeit nicht alle Treiber der WLAN-Hardware die 802.11e Erweiterung. Daher wurde auf eine Modifikation der herkömmlichen WLAN-DCF unter Berücksichtigung des IEEE 802.11e Standards zurückgegriffen. Die Emergency-DCF hat zum Ziel, Zugriffskategorien für die Multimedia Kommunikation, insbesondere im Katastrophenschutz, bereitzustellen.

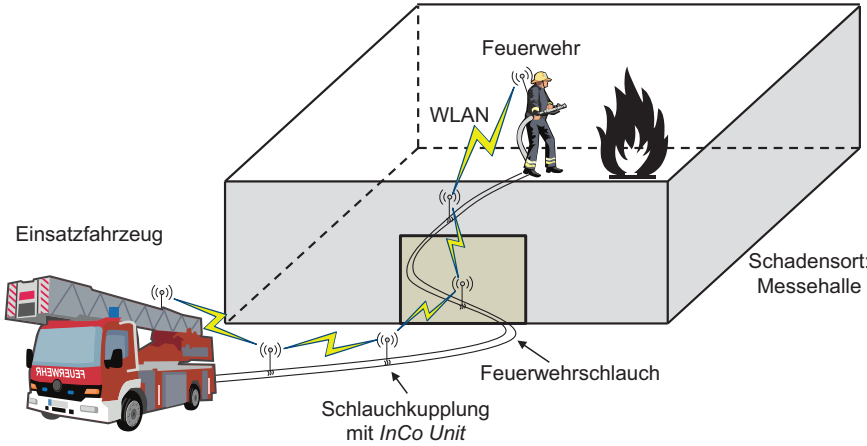


Abbildung 1.3: Anwendergerechter Netzaufbau mittels *InCo Units*

1.3 Anwendergerechter Netzaufbau

In Gesprächen mit Mitarbeitern der Feuerwehr Gelsenkirchen wurde die zusätzliche Arbeit des Ausbringens von *Dropped Units* als störend bezeichnet. Rettungskräfte haben bei einem Einsatz keine Zeit, zusätzlich ein Kommunikationsnetz aufzubauen. Für sie gibt es wichtigere Arbeiten zu erledigen, als ein Kommunikationsnetz aufzubauen.

Ein alternativer Ansatz zum dedizierten Ausbringen ist die Integration der *Dropped Units* in den Arbeitsprozess der Rettungskräfte. Dies kann insbesondere dadurch erreicht werden, dass die Hardware der *Dropped Units* in die Ausrüstungsgegenstände der Rettungskräfte integriert wird. Im Rahmen dieser Arbeit wird die Integration der *Dropped Units* in die Kupplungen von Feuerwehrschläuchen untersucht. Die zwischen die Schlauchkupplungen integrierten *Dropped Units* werden nachfolgend *Inter-Coupling Units*, kurz *InCo Units* genannt. In Abbildung 1.3 ist eine Übersicht zum prozesskonformen Netzaufbau mittels *InCo Units* dargestellt.

Im Rahmen von Feldtests bei der Feuerwehr wurden erste Konzepte entwickelt, wobei *InCo Units* in Schlauchtragekörbe, Drehleitern und Schlauchkupplungen integriert wurden. Letztlich konnte eine Idee der Endanwender aufgegriffen werden. Als ideal wurde seitens der Anwender ein Netzaufbau erachtet, der ohne Änderung ihrer etablierten Prozesse auskommt. Die Wahl für die Integration der *InCo Units* fiel somit auf die Schlauchkupplungen.

Durch die Integration der *InCo Units* in die Kupplungen der Feuerwehrschläuche, die eine standardisierte Länge haben, kann eine regelmäßige Platzierung der *InCo*

Tabelle 1.1: Genormte Längen für Druckschläuche der Feuerwehr (gemäß [18])

Größe	Schlauchlänge in m			
D 25	5	15	-	-
C 42	-	15	20	-
C 52	-	15	20	-
B 75	5	-	20	35
A 110	5	-	20	-

Units angenommen werden. So wird beim Auslegen der Schläuche durch die Feuerwehr gleichzeitig ein Kommunikationsnetz aufgebaut. Die Rettungskräfte können ungehindert ihrer Hauptaufgabe nachgehen und bauen *on-the-fly* ihr Ad-hoc-Netz auf. Dieser anwendergerechte Netzaufbau entspricht auch den Anforderungen der Feuerwehrleute: „Technik folgt Taktik“ [56].

Feuerwehrschläuche gibt es in unterschiedlichen Größen, wobei die Nenngrößen B, C und D bei allen Feuerwehren genutzt werden. In Tabelle 1.1 sind die DIN Längen der einzelnen Schlauchgrößen angegeben [18]. Im Rahmen dieser Arbeit wird angenommen, dass Schläuche der Größe B, die einen Durchmesser von 75 mm und eine genormte Länge von 20 m haben, verwendet werden. Das Kuppeln von Schläuchen der Größe B wird laut Feuerwehr-Dienstvorschrift grundsätzlich von zwei Feuerwehrleuten durchgeführt [2]. Die Integration einer *InCo Unit* bedeutet für zwei Personen nur einen geringen Mehraufwand, der laut Aussagen der Feuerwehrleute nicht als störend empfunden wird.

Die Integration von *InCo Units* zwischen jedes Schlauchstück führt dazu, dass mehr *InCo Units* platziert werden, als für eine WLAN-Abdeckung benötigt werden. Die redundanten *InCo Units* können Interferenzen verursachen, welche den Betrieb des Kommunikationsnetzes stören. Um diese Störungen möglichst gering zu halten, wird im Rahmen dieser Arbeit der Interferenz-Vermeidungs-Algorithmus (IAA) eingeführt [102] (siehe Kapitel 4.2). Dieser Algorithmus sorgt dafür, dass redundante *InCo Units* am Einsatzort deaktiviert werden.

Zusätzlich zum IAA kommen Routing-Algorithmen in den *InCo Units* zum Einsatz, welche die Kommunikationspfade im Netz automatisch finden und aufrechterhalten. Somit kann durch die Integration von *InCo Units* in die Schlauchkupplungen ein selbstkonfigurierendes Kommunikationsnetz anwendergerecht aufgebaut werden.

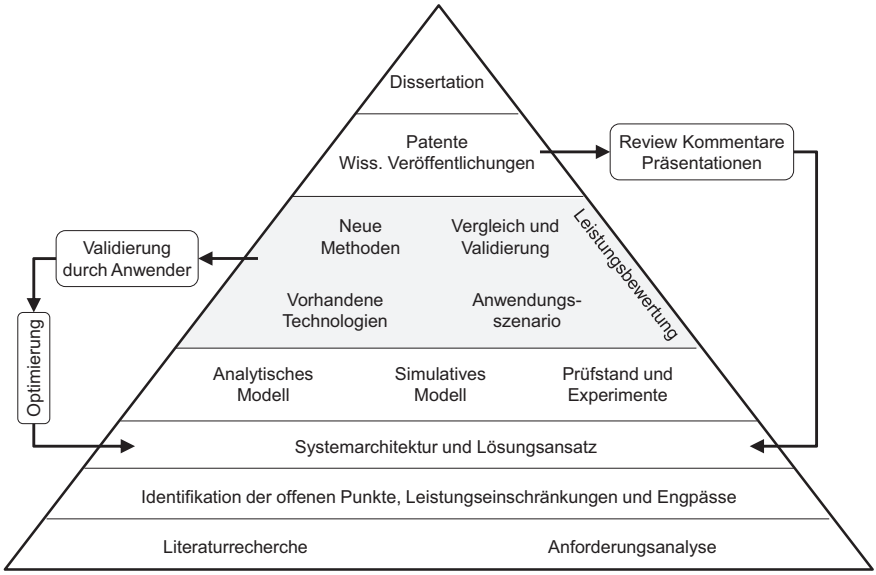


Abbildung 1.4: Wissenschaftliche Vorgehensweise in dieser Dissertation

1.4 Eingesetzte Methoden

Ziel der hier vorliegenden Arbeit ist die Untersuchung, Bewertung und Verbesserung der Zuverlässigkeit eines Ad-hoc-Netzes für den Katastrophenschutz. Das wissenschaftliche Vorgehen in dieser Arbeit ist in Abbildung 1.4 dargestellt. Die Arbeit basiert auf einer Literaturrecherche und Anforderungsanalysen aus mehreren Industrieprojekten.

Nach der Identifikation der offenen Punkte wurde ein Lösungsansatz für das Ad-hoc-Netz für den Katastrophenschutz auf Basis von *Dropped Units* bzw. *InCo Units* erarbeitet. Im Rahmen dieser Arbeit konnten mehrere *Dropped Units* prototypisch realisiert werden. Diese bilden den Prüfstand, welcher für Experimente genutzt wird.

Um die Einschränkungen des Ausmaßes des Prüfstands in Bezug auf die Anzahl der Knoten zu umgehen, wird eine weitere Methode eingesetzt. Basierend auf den Experimenten wurde eine Simulationsumgebung aufgebaut, die eine Untersuchung von größeren Szenarien erlaubt. Diese Simulationsumgebung basiert auf dem OMNeT++ Simulator [91] und der INETMANET Erweiterung.

Für die Leistungsbewertung der WLAN Medien-Zugriffsfunktion (DCF) ist es üblich, ein analytisches Modell basierend auf Markov-Ketten einzusetzen [5]. Eine

Markov-Kette ist ein spezieller stochastischer Prozess, bei dem ein System durch bestimmte Zustände modelliert wird und zukünftige Zustandsübergänge nur von dem aktuellen Zustand abhängig sind. Diese dritte Methode wurde eingesetzt, um die Priorisierung der Rettungskräfte zu untersuchen. Dabei wurden existierende Modelle angepasst und erweitert. Die numerische Berechnung der nicht-linearen Gleichungssysteme, welche zur Ermittlung der Zustandswahrscheinlichkeiten der Markov-Ketten gelöst werden mussten, erfolgte mittels MATLAB [51].

In der Phase der Leistungsbewertung ist das Anwendungsszenario „Brand in einer Messehalle" untersucht worden. Dabei sind neue praxisorientierte Methoden zum Aufbau des Ad-hoc-Netzes eingesetzt worden. Diese wurden verglichen mit existierenden Algorithmen. Dabei fand ständig ein Austausch mit den Endanwendern, insbesondere mit der Feuerwehr Gelsenkirchen, statt. Kommentare sind als Optimierung in die Systemarchitektur eingeflossen.

Auf Basis der Ergebnisse aus der Leistungsbewertung konnten wissenschaftliche Veröffentlichungen und Beiträge zu zwei Patentanträgen entstehen. Die Verbesserungsvorschläge der Reviewer und die Reaktionen bei den Präsentationen sind in den Lösungsansatz eingegangen.

1.5 Zusammenfassung der Beiträge der Arbeit

Unter Berücksichtigung der oben genannten Probleme wurden die folgenden vier Lösungsansätze erarbeitet:

1. Für die ausfallsichere Vernetzung von Rettungskräften am Einsatzort wird der Einsatz von kleinen, tragbaren WLAN-Routern, die im Rahmen dieser Arbeit entstandenen *Dropped Units*, vorgeschlagen.

2. Zur Vereinfachung des Netzaufbaus und der Erhöhung der Akzeptanz beim Endnutzer wird vorgeschlagen, die *Dropped Units* in den Rettungsprozess zu integrieren. Im Rahmen dieser Arbeit wird dieser *rettungsprozessintegrierte Netzaufbau* am Beispiel der Integration von *InCo Units* in die Kupplung von Feuerwehrschläuchen vorgestellt und untersucht.

3. Um die Interferenz von existierenden WLAN-Netzen am Einsatzort zu verringern, wird eine Erweiterung des WLAN-Medienzugriffs DCF unter Berücksichtigung von IEEE 802.11e vorgeschlagen. Diese neue Priorisierungsmethode, *Emergency-DCF* genannt, wird im Rahmen dieser Arbeit beschrieben und bewertet.

4. Um die Interferenzen, die bei der häufigen Platzierung von drahtlosen *InCo Units* entstehen, zu reduzieren, wird die Verwendung eines neuartigen *Interferenz-Vermeidungs-Algorithmus* vorgeschlagen.

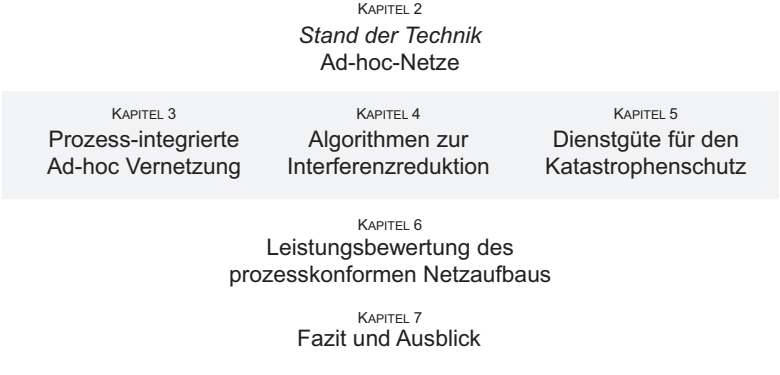


Abbildung 1.5: Aufbau der Dissertation

1.6 Gliederung der Arbeit

Der Aufbau der Dissertation ist in Abbildung 1.5 dargestellt. Der Inhalt der Kapitel wird nachfolgend kurz zusammengefasst.

Kapitel 2 gibt einen Überblick über die für diese Arbeit relevanten Themengebiete. Dabei wird unter anderem der aktuelle Stand der Forschung im Bereich der Kommunikationsnetze für Notfallinformationssysteme vorgestellt. Darüber hinaus wird der IEEE 802.11e Standard präsentiert, der Dienstgüte für Multimedia-Anwendungen erlaubt. Darauf aufbauend wird später die neu eingeführte Dienstgüte für Rettungskräfte entwickelt. Am Ende des Kapitels werden die Methoden der Leistungsbewertung vorgestellt, die im Rahmen dieser Arbeit eingesetzt werden.

Die prozess-integrierte Ad-hoc-Vernetzung auf Basis des neuartigen *Dropped Units*-Konzepts wird in *Kapitel 3* detailliert eingeführt. Es wird dargelegt, wie durch Integration von *InCo Units* in Schlauchkupplungen der Netzaufbau mit dem Arbeitsprozess der Rettungskräfte verknüpft werden kann. Darüber hinaus wird eine Abdeckungsanalyse des Konzepts anhand eines einfachen exemplarischen Szenarios vorgestellt.

Durch die in Kapitel 3 vorgestellte Integration der *InCo Units* in Schlauchkupplungen werden mehr *InCo Units* platziert, als für die Vernetzung notwendig wären. Die redundanten *InCo Units* erzeugen Interferenzen, welche es zu vermeiden gilt. Hierzu werden in *Kapitel 4* Algorithmen zur Interferenzreduktion vorgestellt. Der im Rahmen der Arbeit entstandene neuartige *Interference Avoidance Algorithm* (IAA) wird mit existierenden Algorithmen verglichen.

Um das prozesskonform aufgebaute Kommunikationsnetz nutzen zu können, wird in *Kapitel 5* eine Methode erforscht, die eine anwendungsspezifische Dienstgüte für

Rettungskräfte ermöglicht. Diese Methode basiert auf der Modifikation der IEEE 802.11 *Distributed Coordination Function* (DCF) und einer Erweiterung der im 802.11e Standard gelisteten Dienstgüteklassen um Klassen für Notfallkommunikation. Die neue Priorisierungsmethode Emergency-DCF wird zunächst eingeführt und deren Leistung anschließend analytisch und simulativ untersucht. Abschließend wird ein Experiment vorgestellt, mit dem die Priorisierung in der Praxis untersucht wurde.

In einer abschließenden Simulation wird in *Kapitel 6* die Leistung des prozesskonformen Netzaufbaus anhand von Beispielszenarien untersucht. Dabei werden die beiden Routing-Protokolle OLSR und BATMAN in Kombination mit und ohne IAA miteinander verglichen. Der Parameterraum wird in drei Szenarien untersucht, die eine kleine, mittlere und große Schadenslage darstellen. Durch einen Feldtest bei der Feuerwehr wird das sichere Vernetzungskonzept abschließend validiert.

Kapitel 7 ist das abschließende Kapitel, welches einen kurzen Kommentar zu den Auswirkungen der verschiedenen Beiträge der Arbeit gibt. Es wird ein Überblick der behandelten Themen präsentiert, und insbesondere werden die Vorteile der im Rahmen dieser Arbeit entstandenen bzw. erforschten Themenkomplexe vorgestellt. Abschließend wird eine Richtung für mögliche kommende Arbeiten aufgezeigt und eine Auswahl an noch offenen Fragen formuliert.

2

Ad-hoc-Netze für den Rettungsdienst und Katastrophenschutz

In diesem Kapitel werden der Stand der Technik und die Anforderungen an ein Ad-hoc-Kommunikationsnetz für den Rettungsdienst und den Katastrophenschutz vorgestellt. Zunächst wird dabei allgemein auf die WLAN-Technologie eingegangen, welche die Grundlage für das in dieser Arbeit untersuchte drahtlose Kommunikationsnetz am Einsatzort darstellt. Anschließend werden Routingprotokolle vorgestellt, welche eine selbstkonfigurierende Ad-hoc-Funkversorgung am Einsatzort ermöglichen. Darüber hinaus wird auf Dienstgüte von multimedialen Anwendungen eingegangen, da sie als Grundlage für die Priorisierung der Kommunikation von Rettungskräften dient. Abschließend wird die Methodik vorgestellt, mit der die Leistungsbewertung der entstandenen Konzepte durchgeführt wird.

2.1 Kommunikationsnetze

Die Ad-hoc-Vernetzung von Einsatzkräften an einem Einsatzort setzt ein Kommunikationsnetz voraus, dessen Infrastruktur sehr schnell errichtet werden kann, und das eine sichere und störungsfreie Kommunikation ermöglicht. Die eingesetzte Technologie soll zuverlässig und erprobt sein. Aufgrund der hohen Datenrate, die beispielsweise für Videoübertragungen benötigt wird, muss die Technologie eine hinreichende Datenrate für multimediale Anwendungen zur Verfügung stellen können. Auch der ökonomische Aspekt muss berücksichtigt werden, da die Technologie bei Feuerwehren und im Katastrophenschutz eingesetzt werden soll und durch kommunale Haushalte finanziert wird, welche zumeist nur über eingeschränkte finanzielle Mittel verfügen.

Unter Berücksichtigung aller Anforderungen wird im Rahmen dieser Arbeit die WLAN-Technologie nach dem Standard IEEE 802.11 für die Ad-hoc-Vernetzung von Einsatzkräften untersucht und angepasst.

Im Rahmen dieser Arbeit sind WLAN-Router entstanden, welche die Anforderungen der Rettungskräfte aus Sicht des Kommunikationsnetzes adressieren. Mit den *Dropped Units* genannten WLAN-Routern ist der Aufbau eines Ad-hoc-Kommunikationsnetzes möglich.

2.1.1 Historischer Abriss des Behördenfunks

Die Fähigkeit über weite Distanzen zu kommunizieren war für koordinierte Operationen schon immer notwendig. Einsatzleiter müssen Einsatzkräfte im Feld führen und gleichzeitig immer ein aktuelles Bild der Lage haben. In der *Feuerwehrdienstverordnung 100* wird ein dreigliedriger Führungsvorgang beschrieben [1]. Zunächst wird die Lage erkundet, wobei die Informationsgewinnung im Vordergrund steht. Anschließend wird der Einsatz geplant, wobei die Lage zunächst beurteilt und daraufhin ein Entschluss gefasst wird. Abschließend werden den Einsatzkräften Befehle erteilt, um den beschlossenen Einsatzplan umzusetzen.

Bei einer sehr großen Schadenslage müssen Befehle auch über weite Entfernungen erteilt werden. Bevor Befehle in Form von elektrischen Signalen kabelgebunden übertragen werden konnten, mussten sie beispielsweise per Meldereiter übermittelt werden. Die kabelgebundene Kommunikation, welche zunächst per Morsecode und später per Fernschreiber betrieben wurde, kam jedoch für Einsätze in Gebieten, in denen keine Infrastruktur zur Verfügung stand, nicht in Frage. Revolutionär war hier die Einführung der Kommunikation zwischen Einsatzleiter und Feldkräften mittels tragbarer Zwei-Wege-Funkgeräte, sog. Walkie-Talkies. Im Bereich der Behörden mit Sicherheitsaufgaben war solch ein Funkgerät erstmals 1923 bei der Polizei in Victoria in Australien im regelmäßigen Gebrauch [26]. Zehn Jahre später, im Jahr 1933, wurden alle Streifenwagen der Polizei von Bayonne in New Jersey, USA, mit Zwei-Wege-Funkgeräten ausgestattet [13]. Aufgrund des erfolgreichen Einsatzes der Funkgeräte in Bayonne wurden alle Streifenwagen in den USA standardmäßig mit Funkgeräten bestückt. Ab 1935 veröffentlicht der Verband der Verbindungsbeamten für Aufgaben der öffentlichen Sicherheit (engl. *Association of Public Safety Communications Officials* (APCO)) monatlich das APCO Bulletin Journal. In den 1970er Jahren entwickelt dieser Verband den APCO-16 Standard, welcher die Eigenschaften und Möglichkeiten von Bündelfunknetzen für Sicherheitsaufgaben beschreibt, wobei zunächst das 800 MHz Band lizenziert wurde. In den USA arbeiten heute noch immer zahlreiche Systeme bei 806-824 MHz/ 851-869 MHz, das auch als 800 MHz Band bekannt ist.

In Deutschland hat eine ähnliche Entwicklung stattgefunden. Ein Grund für die Standardisierung war die unzureichende Kommunikationssituation während des verheerenden Waldbrandes in der Lüneburger Heide im Jahre 1975 [80]. An dem Rettungseinsatz waren 15000 Feuerwehrleute aus dem gesamten Bundesgebiet beteiligt. Im Einsatz waren im Vergleich zu Vielkanalgeräten die günstigeren Wenigkanal-Funkgeräte, wobei jede Feuerwehr nur ihren Heimatkanal bestückt hatte. Somit war eine Kommunikation der Feuerwehren untereinander nicht oder nur sehr eingeschränkt möglich. Als Folge konnten eingeschlossene Feuerwehren keinen Notruf absetzen, und zahlreiches Material und fünf Feuerwehrleute fielen den Flammen zum Opfer. Dies führte 1976 zur Einführung einheitlicher Funkanlagen bei Behörden und Organisationen mit Sicherheitsaufgaben (BOS) [25]. Die im

Quelle: http://funkportal24.de/jpg/Zentrale.jpg

Abbildung 2.1: Fernmeldezentrale: Führungstelle mit Sprechfunk- und Fernsprechbetrieb

BOS-Kontext eingesetzten Funkgeräte (FuG), bzw. die neu zugelassenen Funkanlagen, sollten ab diesem Zeitpunkt laut Punkt 7 des Beschluss der Sitzung der Innenministerkonferenz (IMK April 1976) den „Technischen Richtlinien“ BOS (TR BOS) entsprechen, also alle vorgesehenen BOS-Kanäle empfangen können. Das damals eingeführte Kanalraster (20 kHz) wird noch heute beim analogen BOS-Funk verwendet. In Abbildung 2.1 ist eine Führungsstelle mit Sprechfunk- und Fernsprechbetrieb einer Fernmeldezentrale abgebildet. Interessant sind auch die Landkarten an den Wänden, auf die mittels Magneten Taktische Zeichen angebracht wurden.

Seit 2006 wird der digitale Behördenfunk in Deutschland eingeführt (*Terrestrial Trunked Radio* - TETRA), der eine maximale Datenrate von 10,8 kbit/s zur Verfügung stellt [9]. Der Digitalfunk wird im Rettungsdienst hauptsächlich für die Sprachkommunikation genutzt. In Abbildung 2.2 ist eine exemplarische Kommunikationsskizze des Bayerischen Roten Kreuzes (BRK) dargestellt. In der Skizze ist oben links der Einsatzleiter am Einsatzort eingezeichnet, der hierarchisch nach oben per Telefon und Funk mit der Integrierten Leitstelle (ILS), also der Zentrale für die Alarmierung und Koordinierung von Feuerwehr und Rettungsdienst, verbunden ist. Am Einsatzort selbst ist der Einsatzleiter mit den einzelnen Einsatzabschnitten per Sprechfunk verbunden. Dabei stellt der *BOS-Kanal 42 GU* einen Engpass dar. Dieser Sprachkanal wird insbesondere für die regelmäßige Aktualisierung von Informationen an den Einsatzleiter eingesetzt. Nach BRK sind wichtige Informationen in diesem Kontext z.B. verfügbare Kapazitäten der Ret-

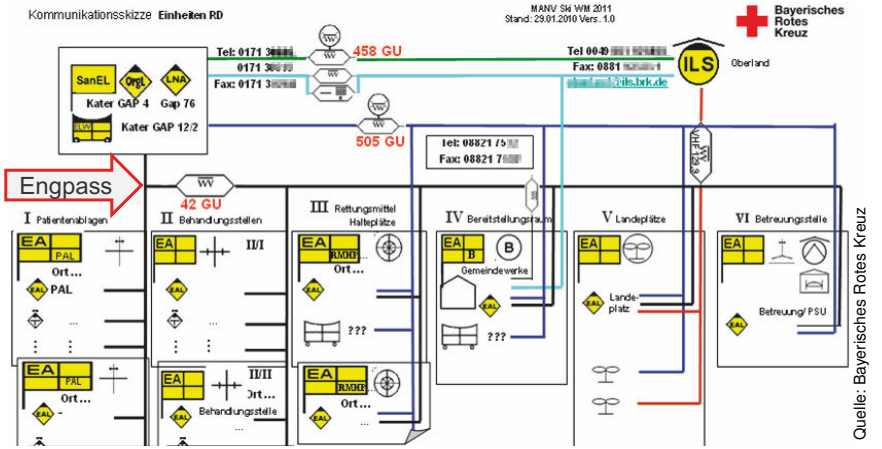


Abbildung 2.2: Kommunikationsskizze des BRK Rettungsdienstes

tungsmittel und die Anzahl der Patienten. Im Gespräch mit dem BRK ist der Wunsch nach einer digitalen Übertragung dieser Daten geäußert worden.

Die geringen Datenraten des digitalen Behördenfunks (max. 10,8 kbit/s pro Zeitschlitz) führen dazu, dass ein zusätzliches Kommunikationsnetz benötigt wird, wenn multimediale Daten zwischen den Rettungskräften untereinander und zwischen dem Einsatzleiter und Feldkräften ausgetauscht werden sollen. Der digitale Behördenfunk ist für eine reine Sprachübertragung optimiert. Die zusätzliche Übertragung von einsatzrelevanten Informationen bringt das Netz an die Kapazitätsgrenze bzw. übersteigt diese.

Der Aufbau eines derartigen Netzes, welches die Nutzung von multimedialen Diensten für den Katastrophenschutz ermöglicht, ist Fokus dieser Arbeit. Nachfolgend werden einige Dienste vorgestellt, die den Austausch von multimedialen Daten im Katastrophenschutz ermöglichen.

2.1.2 Wireless LAN

Das im Rahmen dieser Arbeit untersuchte Ad-hoc-Kommunikationsnetz für Rettungskräfte basiert auf dem Wireless LAN Standard IEEE 802.11-12 [40]. Relevante Grundlagen werden im Folgenden kurz vorgestellt. Vertiefende Informationen findet der interessierte Leser z.B. bei *Rech* [68].

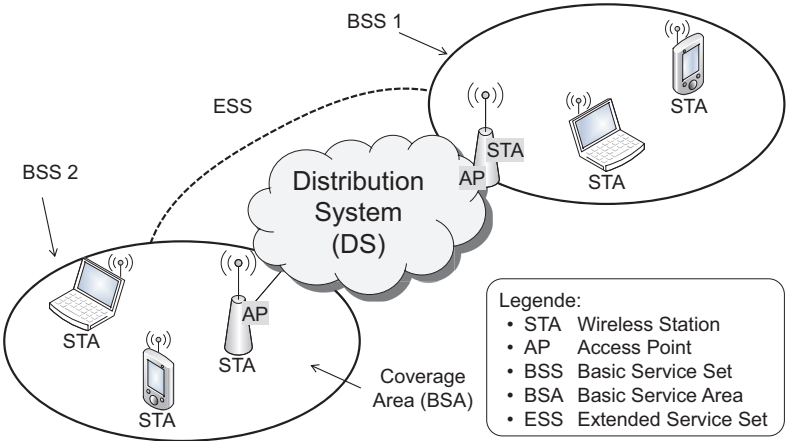


Abbildung 2.3: Netzarchitektur bei IEEE 802.11

Netzarchitektur

Die Architektur des Kommunikationsnetzes bei IEEE 802.11 ist in Abbildung 2.3 dargestellt. Im Standard werden WLAN-Knoten *Wireless Station* (STA) genannt. Mindestens zwei STAs bilden ein drahtloses Kommunikationsnetz, welches *Basic Service Set* (BSS) genannt wird. Der Abdeckungsbereich (engl. *Coverage Area*) des WLAN-Funks wird meistens als ovale Fläche gezeichnet und *Basic Service Area* (BSA) genannt. Ein BSS kann mittels eines *Access Point* (AP) an ein weiteres Netz, zumeist ein Ethernet, angeschlossen werden. Dieses zusätzliche Netz wird als *Distribution System* (DS) bezeichnet und kann z.B. das Internet sein. Werden zwei BSS über ein DS miteinander verbunden, so werden die verbundenen BSS *Extended Service Set* (ESS) genannt.

2.1.3 Routingprotokolle für Ad-hoc-Netze

Soll ein WLAN-Ad-hoc-Netz ein Gebiet abdecken, welches die maximale Kommunikationsdistanz von zwei WLAN-Knoten übersteigt, so muss die Kommunikation über Knoten in der Mitte des Gebiets weitergeleitet werden, wenn zwei weit entfernte Knoten miteinander kommunizieren möchten. Das Besondere bei der Vermittlung von Paketen in Ad-hoc-Netzen vom Sender zum Empfänger ist, dass die Netztopologie sich ständig ändern kann. Sowohl Hosts als auch Router können mobil sein. Beispielhaft seien einige Situationen aufgeführt, bei denen dieser Fall unter anderem auftreten kann:

- Rettungskräfte bei einer Großschadenslage, bei dem die Infrastruktur zerstört wurde [66].
- Eine Versammlung von Personen mit Notebooks in einem Gebiet ohne IEEE 802.11 Infrastruktur (keine Access Points vorhanden).
- Ein Schwarm von Flugrobotern bei einem kooperierenden Erkundungsflug ohne Infrastruktur [15].

Flächendeckende Funknetzversorgung

Für die flächendeckende Funknetzversorgung mittels WLAN sind mehrere Ansätze möglich. Nachfolgend werden kurz drei mögliche Ansätze beschrieben.

Einfacher, kabelgebundener Ansatz

Die leistungsfähigste Vernetzung basiert auf kabelgebundener Vernetzung von Access Points am Einsatzort. Dies stellt zugleich die unpraktischste Art der Vernetzung dar, weil eine Verkabelung mit Zeitverlust verbunden ist. Daher wird nicht weiter auf diese Vernetzungsart eingegangen.

Wireless Distribution System

Die einfachste Möglichkeit zur kabellosen Vernetzung besteht darin, den Abdeckungsbereich eines zentralen *Access Points* mit Hilfe von weiteren *Access Points* zu vergrößern, wobei das *Wireless Distribution System* (WDS) eingesetzt wird [109]. In der Regel werden dabei aus Kostengründen *Single Radio Access Points* eingesetzt. Dabei nutzen sowohl die Einsatzkräfte als auch das *Backbone* Netz, also die drahtlose Verbindung der einzelnen Access Points, die gleiche Frequenz für die Kommunikation. Dies führt schon bei relativ wenigen Clients und kleinen Netzen zu erhöhter Interferenz.

Besser geeignet sind hier *Dual Radio Access Points*, also Geräte, die gleichzeitig auf zwei unterschiedlichen Frequenzen, bzw. WLAN-Kanälen, senden können [110]. Der eine Kanal wird für die Kommunikation der Clients und der andere für das *Backbone* verwendet. Die Konfiguration des Netzes ist relativ einfach. Es wird ein Kanal für das *Backbone* und ein Kanal für die Kommunikation mit den Endgeräten konfiguriert. Zusätzlich werden WPA2 Schlüssel für die Verschlüsselung und bei allen Access Points die gleiche SSID eingetragen. Anschließend wird WDS aktiviert.

Wireless Mesh-Netze
Wireless Mesh-Netze (WMN) dienen zur drahtlosen Vernetzung von Endgeräten in großen Szenarien. Ähnlich wie beim WDS bilden quasi stationäre Knoten das *Backbone* des Netzes. Voneinander entfernte Knoten (beispielsweise Rettungskräfte) nutzen das *Backbone* um miteinander kommunizieren zu können. Die Vernetzung basiert bei WMN nicht auf dem WDS, sondern auf speziellen Routing-Protokollen, welche den Kommunikations-Pfad zwischen zwei entfernten Knoten finden und aufrechterhalten. Die Erweiterung IEEE 802.11s standardisiert die Mesh-Funktionalität von WLAN (siehe [30] und [**?**]).

Routing in WMN stellt besondere Anforderungen an das Routing-Protokoll, da sich die Topologie des Netzes ständig verändert. Daher müssen auch die Routen, auf denen kommuniziert wird, ständig den Gegebenheiten angepasst werden. Der Zeitpunkt dieser Anpassung kann entweder direkt vor dem Versenden der eigentlichen Information sein, oder die Anpassung wird kontinuierlich durchgeführt. Diese beiden unterschiedlichen Arten der Anpassung dienen dazu, Routing-Protokolle für Ad-hoc-Netze in zwei Kategorien einzuteilen. Wird die Route kurz vor der Übertragung der eigentlichen Information erstellt, wird dies reaktives Routing genannt. Wird stattdessen die Route kontinuierlich aktualisiert, so wird dies proaktives Routing genannt.

- Proaktive Protokolle senden periodische Nachrichten per Broadcast an die Umgebung aus, um zu jeder Zeit eine Verbindung aufrechtzuerhalten. Der Vorteil dieser Methode liegt darin, dass Nachrichten sehr schnell versendet werden können, weil ein Pfad existiert, der immer aufrechterhalten wird. Nachteil ist das hohe Datenaufkommen aufgrund der vielen periodischen Nachrichten, welche die maximale Datenrate des WMNs senken. Ein weiterer Nachteil entsteht bei sehr dynamischen Szenarien, bei denen es zu häufigen Unterbrechungen der Routen kommt, weil dadurch die Routing-Tabellen nicht mehr aktualisiert werden können. Daher ist es wichtig, dass durch häufiges Versenden der periodischen Nachrichten die Routen möglichst aufrechterhalten werden. Beispiele für proaktive Protokolle sind OLSR und BATMAN [12], [3], [44].
- Reaktive Protokolle suchen bei Bedarf einen Pfad zwischen zwei Kommunikationspartnern. Vorteil hierbei ist der geringe Overhead, der durch das Protokoll verursacht wird. Die maximale Datenrate des Netzes wird kaum beeinträchtigt. Anderseits entsteht eine Verzögerung bei der Pfadsuche, wenn zwei Knoten zum ersten Mal miteinander kommunizieren wollen, oder eine Änderung der Netztopologie eingetreten ist. Ein Beispiel für ein reaktives Protokoll ist AODV [61].
- Hybride Protokolle wie das im Standard IEEE 802.11s definierte HWMP nutzen beide Methoden. Jeder Knoten im Netz hält ständig einen Pfad zum so genannten Wurzelknoten aufrecht, der häufig an das Internet angeschlossen ist. So können die Knoten jederzeit schnell mit dem Internet kommunizieren.

Wollen zwei Knoten innerhalb des WMNs miteinander kommunizieren, wird der Kommunikations-Pfad mittels einer reaktiven Methode gesucht [30], [10].

Die Knoten eines WMNs lassen sich aus beliebiger Hardware konfigurieren, welche die Routingprotokolle unterstützt. Aus Energiespargründen bietet sich die Verwendung von ARM-basierten eingebetteten Systemen an, welche mit dem Linux Betriebssystem betrieben werden. Für Linux existiert eine Reihe von Routing-Protokollen, die sich für den Zweck der Vernetzung von Rettungskräften am Einsatzort eignen. In den neueren Linux Versionen (Kernel > 3.2) ist BATMAN-Advanced, ein leistungsstarkes, proaktives Routing-Protokoll, bereits integriert.

Im Rahmen dieser Arbeit wird in den Untersuchungen in Kapitel 6 auf die Protokolle BATMAN und OLSR zurückgegriffen. Die Funktionsweise dieser beiden Protokolle wird nachfolgend kurz erläutert.

BATMAN

Eine einfache pragmatische Herangehensweise für Mesh-Routing in großen, statischen Mesh-Netzen wird von BATMAN bereitgestellt [44]. Bei BATMAN senden alle Knoten periodisch so genannte *Originator Messages (OGMs)* per Broadcast an ihre Nachbarn. OGMs sind 52 Bytes groß, inklusive UDP und IP Overhead und beinhalten mindestens die Originator-IP, eine Sequenznummer und eine Time-To-Live (TTL). Wird eine OGM von einem fremden Knoten empfangen, so wird diese OGM erneut per Broadcast versendet und zuvor die TTL des OGM-Pakets dekrementiert. Darüber hinaus erhöht der Empfänger den Zähler für seine Nachbar-Originator-Paare [73].

Diese OGMs werden genutzt, um den nächstbesten Hop in Richtung des Ziels zu finden. Um die beste Route zum Ziel zu finden, zählt BATMAN die Anzahl der OGMs, die von dem Knoten abgesendet und von seinen Nachbarn empfangen wurde. Es wählt dann den Nachbarn als nächsten Hop, von dem es die höchste Anzahl von OGMs innerhalb eines Zeitfensters empfangen hat. Die Anzahl der empfangenen OGMs ist also gleichbedeutend mit der Qualität der Verbindung. Auf diese Weise kennt jeder Knoten zwar nicht die gesamte Route zwischen Quelle und Ziel, aber er kennt den Nachbarn, an den ein Paket weitergeleitet werden muss, um das Ziel zu erreichen.

Delosieres et al. verwenden BATMAN in Katastrophenschutzszenarien [17]. Sie schlagen einen *Store-and-Forward* Mechanismus vor, der dafür sorgt, dass Pakete bei kurzzeitigen Verbindungsunterbrechungen zwischengespeichert werden. Darüber hinaus werden bei *Delosieres* die OGMs von BATMAN mit Pheromonen aus dem Tierreich verglichen. So nutzen Ameisen Pheromone, um den Weg zwischen ihrem Bau und einer Futterstelle zu markieren. Je öfter eine Ameise einen Pfad abläuft, so intensiver wird die Pheromonspur. Dies führt dazu, dass noch mehr Ameisen diesen Pfad wählen. Genauso verhält es sich bei BATMAN und den

OGMs. Je mehr OGMs erfolgreich zwischen zwei Knoten ausgetauscht werden, desto höher ist die Wahrscheinlichkeit, dass Pakete über diese Strecke geroutet werden.

Neben BATMAN, welches als klassisches Layer-3 Routing-Protokoll arbeitet, gibt es *BATMAN Advanced*, welches auf Layer-2 funktioniert. Der Hauptunterschied zwischen BATMAN und BATMAN Advanced ist die Verwendung von MAC- anstatt von IP-Adressen für das Routing. Diese Eigenschaft befähigt BATMAN Advanced auch IPv6 zu unterstützen und ist somit zukunftssicher.

Optimized Link State Routing - OLSR

Das von *Clausen et al.* [12] im RFC 3626 vorgeschlagene *Optimized Link State Routing* (OLSR) ist ein häufig eingesetztes proaktives Routing-Protokoll. Knoten, die dieses Protokoll verwenden, halten ständig die Topologie-Information des gesamten Netzes auf einem aktuellen Stand. Dies basiert auf periodisch ausgetauschten *link-state*-Nachrichten, so genannten *HELLO*-Nachrichten. Um den negativen Effekt des simplen Flutens dieser Nachrichten auf die Gesamtleistung des Netzes zu minimieren, nutzt OLSR das *Multi Point Relaying* (MPR), was das Hauptkonzept dieses Protokolls ist. Beim MPR wählen die Knoten nur einige Nachbarknoten aus, welche Daten im Netz als *Relay* weiterleiten, anstatt dass jeder Knoten im Netz als *Relay* fungiert. Die *Relay*-Knoten werden MPR genannt. Jeder Knoten, der kein MPR ist, kann zwar jedes Paket in seinem Empfangsbereich lesen und verarbeiten, leitet es aber nicht weiter.

Die Wahl, welcher Knoten MPR ist, basiert auf einer Liste der 1-Hop-Nachbarn, die periodisch per Broadcast gesendet wird. Jeder Knoten definiert von dieser Liste eine Untermenge seiner 1-Hop-Nachbarn, die all seine 2-Hop-Nachbarn abdecken. Diese Untermenge sind die MPRs. Die Verwendung von MPRs reduziert den negativen Effekt des Flutens von Kontrollnachrichten, da nur noch die MPRs diese Nachrichten weiterleiten. Je größer und dichter ein Netz ist, also jeder Knoten mehrere 1-Hop und 2-Hop-Nachbarn hat, desto besser funktioniert diese Optimierung.

OLSR nutzt zwei Arten von Kontrollnachrichten: HELLO und Topology Control (TC). HELLO-Nachrichten werden verwendet, um die Verbindung zu direkten Nachbarn zu finden und ihre Verbindungsqualität zu ermitteln. Darüber hinaus werden über die HELLO-Nachrichten die MPRs ermittelt. Mit den TC-Nachrichten werden die Topologieinformationen ausgetauscht. Für die Pfadauswahl nutzt OLSR den kürzesten Pfad zwischen Quelle und Ziel und verwendet dabei die *hop-count*-Metrik, bei der die Anzahl der benötigten Hops gezählt wird.

Ein guter Überblick zu den Parametern und deren Einfluss auf den Durchsatz wird bei *Huang et al.* gegeben [34]. *Naudts et al.* nutzen OLSR für das Routing in WMNs bei Großschadenslagen [57].

Quelle: Automatic relay dispenser [50]

Abbildung 2.4: Automatischer Relayabwurf durch am Gürtel befestigten Relay-Spender [50]

2.1.4 Existierende Vernetzungskonzepte

Um die Rettungskräfte an einem Einsatzort miteinander zu vernetzen, existieren einige Ansätze. Ein WLAN-Netz an einem Einsatzort kann mittels batteriebetriebener WLAN-Router verfügbar gemacht werden [7]. Dazu müssen diese jedoch zuvor von einer Rettungskraft am Einsatzort aufgestellt werden. Ein weiterer Ansatz sieht vor, das Kommunikationsnetz mittels kleiner Router-Knoten aufzubauen, die immer dann aus einem am Gürtel befestigten Spender abgeworfen werden, wenn eine definierte Empfangssignalstärke unterschritten wird [50]. Da hierfür sehr kleine Hardware benötigt wird, basiert das Konzept auf der ZigBee-Technologie. Neuerdings wird erforscht, inwiefern Flugroboter bei der Vernetzung von Rettungskräften am Boden eingesetzt werden können. Die Flugroboter können mit WLAN-Routern ausgestattet werden und damit ein Mesh-Netz über dem Einsatzort aufbauen [64].

Sollen *Relays* von Rettungskräften während des Einsatzes ausgebracht werden, so sollte dieser Ausbringungsprozess die Rettungskraft möglichst nicht an der Arbeit hindern. Hier setzen *Liu et al.* [50] mit ihrem automatischen Abwurfsystem

an. Dieses System wird an einen Gürtel befestigt und wirft automatisch ein Kommunikationsrelay ab, sobald eine bestimmte Signalqualitätsschwelle unterschritten wird. In Abbildung 2.4 ist der am Gürtel befestigte Spender dargestellt (Markierung 1). Auf dem Boden befinden sich bereits zwei *Relays* (Markierung 2 und 3). *Liu et al.* nutzen ZigBee [39] für ihre Untersuchungen. Daher sind die *Relays* relativ klein. Das Referenzszenario für den Einsatz von ZigBee ist die energieeffiziente Übertragung von Sensordaten mit geringen Datenraten (250 kbit/s).

Im Rahmen dieser Arbeit werden Dienste als Anforderungen an das Kommunikationsnetz angenommen, die wesentlich höhere Datenraten erfordern. Daher wird ZigBee nicht weiter behandelt. Außerdem ist das Einsammeln der *Relays* nach dem Einsatz unpraktisch, und das Zurücklassen der Hardware am Einsatzort zu teuer.

Neben den in der Forschung befindlichen Technologien gibt es bereits kommerzielle Systeme, die aber teuer und eher für den stationären Einsatz geeignet sind. Ein Beispiel hierfür ist der *Highly Mobile Network Node*, kurz HiMoNN, der Firma IAGB [35].

2.2 Dienstgüte für Multimedia Anwendungen

Im Kontext von Katastrophenschutzszenarien ist die Unterstützung von Dienstgüte wichtig, da die Übertragung von bestimmten Diensten Vorrang vor anderen Diensten haben können. Im Rahmen dieser Arbeit wird WLAN Kommunikation nach IEEE 802.11 für die Übertragung dieser Dienste verwendet, wobei im Kontext von Dienstgüte IEEE 802.11e eine große Rolle spielt. Daher wird nachfolgend kurz auf IEEE 802.11e eingegangen.

Die hier beschriebenen Grundlagen für die Unterstützung von Dienstgüte für multimediale Anwendungen im WLAN basieren auf [93]. Durch die Dienstgüteerweiterung von IEEE 802.11e werden neue Funktionen in der Netzarchitektur eingeführt. In IEEE 802.11e werden Stationen als *QoS supporting Stations* (QSTAs) bezeichnet, welche Dienstgütefunktionen den ursprünglichen (engl. *legacy*) IEEE 802.11 Stationen (STAs) hinzufügt.

2.2.1 Medienzugriffskontrolle

Der Medienzugriff bei 802.11e findet entweder zentral gesteuert, oder verteilt statt. Da im Rahmen dieser Arbeit ein Ad-hoc-Netz für die Kommunikation eingesetzt wird, bei dem keine zentrale Instanz vorgesehen ist, ist der zentral gesteuerte Ansatz von 802.11e (die sogenannte *Hybrid Coordination Function*) hier nur der Vollständigkeit halber angeführt.

Wichtiger im Zusammenhang mit Ad-hoc-Netzen ist der verteilte Medienzugriff, der in 802.11e *Enhanced Distributed Channel Access* (EDCA) genannt wird.

Darüber hinaus wird in IEEE 802.11e ein Zeitintervall eingeführt, währenddessen Stationen ein exklusives Übertragungsrecht haben, *Transmission Opportunity* (TXOP) genannt. TXOPs, die von der EDCA erhalten wurden, haben eine begrenzte Dauer, die $TXOP_{limit}$ genannt wird. Standard STAs ignorieren dieses neue Informationsfeld und berücksichtigen diese Einschränkung nicht.Nachfolgend wird die EDCA detaillierter vorgestellt.

2.2.2 Enhanced Distributed Channel Access (EDCA)

Um Dienstgüte zu unterstützen, führt die EDCA vier Zugriffskategorien (ACs) ein. Jede AC hat eine korrespondierende *Backoff*-Instanz. Die vier *Backoff*-Instanzen einer 802.11e-Station arbeiten parallel und setzen den wettbewerbsbasierten Zugriff unter Berücksichtigung der jeweiligen Zugriffskategorie um. Die vier Zugriffskategorien (ACs) von 802.11e, AC_BK (*background*), AC_BE (*best effort*), AC_VI (*video*) und AC_VO (*voice*), sind von den Nutzerprioritäten abgeleitet, die im Anhang H.2 des IEEE 802.1D [36] definiert sind. Die Priorisierung zwischen den vier *Backoff*-Instanzen wird durch unterschiedliche AC-spezifische Parameter erreicht, die im Folgenden als EDCA-Parametersätze bezeichnet werden. Diese EDCA-Parametersätze verändern den *Backoff*-Prozess durch individuelle Wartezeiten zwischen den Datenrahmen und unterschiedliche Größen der Wettbewerbsfenster pro AC, was eine wahrscheinlichkeitsbasierte Priorisierung ermöglicht, welche nachfolgend erläutert wird. Die EDCA-Parameter von jeder *Backoff*-Instanz werden durch den HC definiert und können sich über die Zeit ändern. Nur der QAP kann diese Parameter in Abhängigkeit des Verkehrs in der QBSS anpassen. Die EDCA-Parameter werden daher per *Broadcast* durch die *information fields* in den *Beacon*-Rahmen verteilt. Damit die Priorisierung funktioniert, müssen alle *Backoff*-Instanzen in einer QBSS identische EDCA-Parameter verwenden. Im Falle einer IQBSS ist der *Beacon holder* für die Festlegung des EDCA-Parametersatzes verantwortlich. Jede *Backoff*-Instanz innerhalb einer QSTA wetteifert individuell um das Erlangen einer TXOP. Falls mehrere *Backoff*-Instanzen einer QSTA gleichzeitig auf einen *Slot* zugreifen wollen, so wird eine interne virtuelle Kollisionsauflösung durchgeführt: Die *Backoff*-Instanz mit der höchsten AC darf in dem *Slot* übertragen, während sich die übrigen *Backoff*-Instanzen so verhalten, als ob eine Kollision in dem *Slot* aufgetreten wäre. Trotzdem kann der Übertragungsversuch der höchsten AC mit den Rahmen einer anderen Station kollidieren.

2.2.3 Arbitration Interframe Space (AIFS)

Nachdem eine *Backoff*-Instanz festgestellt hat, dass der Kanal für einen *Arbitration Interframe Space* (AIFS) frei ist, beginnt sie mit dem Herunterzählen des *Backoff*-

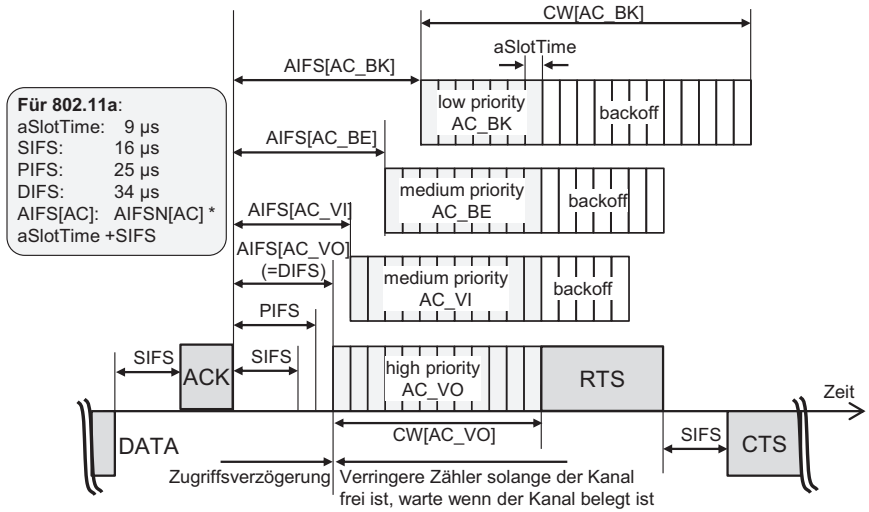


Abbildung 2.5: EDCA Timing-Diagramm für 802.11e (nach [93])

Zählers. Der AIFS hat mindestens die Dauer eines *DCF Interframe Spaces* (DIFS) und hängt von der entsprechenden AC ab, wie im *Timing-Diagramm* in Abbildung 2.5 für die vier ACs von 802.11e dargestellt ist. Um die Abhängigkeit des AIFS von der entsprechenden AC hervorzuheben, wird sie nachfolgend mit AIFS[AC] angegeben. Der *Short Interframe Space* (SIFS) ist der kürzeste *Interframe Space* von 802.11. Es wird für die Rahmen zwischen den RTS/CTS DATA/ACK-Sequenzen genutzt. Der *PCF Interframe Space* (PIFS) wird von der PCF genutzt, um auf den Kanal zuzugreifen. Die *Arbitration Interframe Space Number* (AIFSN), welche für jede AC in Tabelle 2.1 definiert ist, verlängert den AIFS[AC] nach der Formel

$$AIFS[AC] = AIFSN[AC] \cdot aSlotTime + aSIFSTime$$

Je kleiner das AIFSN[AC], desto höher ist die Zugangspriorität. Den frühesten Kanalzugriff bekommt somit die Kategorie *Voice*. Die Priorisierung wird über unterschiedliche Werte für das Wettbewerbsfenster erreicht, was nachfolgend beschrieben wird.

2.2.4 Größe des Wettbewerbsfensters

Das Wettbewerbsfenster (engl. *Contention Window - CW*) der *Backoff*-Prozedur wird ebenfalls in 802.11e für die Bereitstellung von Prioritäten eingesetzt. Sein Minimum CWmin[AC] und sein Maximalwert CWmax[AC] hängen von der AC ab, wie in Abbildung 2.5 dargestellt. Allgemein gilt, dass der kleinste Wert für

Tabelle 2.1: Standardwerte für EDCA Parameter basierend auf [40]. Werte, die von der Bitübertragungsschicht abhängen, sind mit einem Stern * markiert. Hier sind 802.11b/802.11a ausgewählt.

AC	CWmin	CWmax	AIFSN	TXOPlimit*
AC_BK	CWmin*	CWmax*	7	0/0
AC_BE	CWmin*	CWmax*	3	0/0
AC_VI	(CWmin*+1)/2-1	CWmin*	2	6.016/3.008 ms
AC_VO	(CWmin*+1)/4-1	(CWmin*+1)/2-1	2	3.264/1.504 ms

CWmin[AC] = 0 und der größte Wert für CWmax[AC] = 32767 ist. Die Standardwerte sind in Tabelle 2.1 aufgeführt. Beispielsweise sind die Werte für einen 802.11a *PHY Layer* als CWmin=15 und CWmax=1023 definiert. Ein kleiner CWmin[AC]-Wert führt zu einer hohen Priorisierung des Zugriffs. Er führt jedoch auch zu einer erhöhten Kollisionswahrscheinlichkeit, wenn mehrere *Backoff*-Instanzen derselben AC innerhalb einer QBSS um den Kanalzugriff wetteifern. Falls die Übertragung eines Rahmens fehlschlägt, so wird das Wettbewerbsfenster so lange vergrößert, bis der Wert CWmax[AC] erreicht wird. Ein kleines CWmax[AC] ergibt eine hohe Priorität beim Kanalzugriff. Die *Backoff*-Prozedur einer AC wird ausgelöst, falls eine Übertragung fehlschlägt oder es zu einer virtuellen Kollision kommt, die durch einen gleichzeitigen internen Übertragungsversuch von mehreren ACs verursacht wurde. Die 802.11e *Backoff*-Instanz wählt ähnlich wie die Standard DCF eine gleichverteilte Zufallszahl als Zähler.

Vergleichbar zur ursprünglichen DCF startet der 802.11e *Backoff*-Zähler bei einer gleichverteilten Zufallszahl aus dem Intervall [0,CW_i[AC]], welche dann bei jedem Takt um eins verringert wird. Die Größe des Wettbewerbsfensters $CW_i[AC]$ des *Backoff-Stages* i ist definiert als:

$$CW_i[AC] = min\left[2^i(CW_{min}[AC]+1)-1, CW_{max}[AC]\right]$$

Die strenge Priorisierung geht verloren, wenn hoch priorisierte *Backoff*-Instanzen ihr Wettbewerbsfenster nach einer Kollision vergrößern, während niedrig priorisierte *Backoff*-Instanzen keine Kollisionen erfahren. Der relative Unterschied zwischen den Wettbewerbsfenstern von unterschiedlichen ACs, die für die Priorisierung wichtig sind, geht in einem solchen Fall verloren. Ursprüngliche Stationen, also IEEE 802.11a Stationen (STAs), haben ein CWmin = 15, CWmax = 1023 und eine frühestmögliche Kanalzugriffszeit von AIFS = DIFS = 34 μs. Eine 802.11e QSTA hat eine höhere Priorität als ursprüngliche STAs durch das Setzen ihres CWmin[AC] $<$ 15 und CWmax [AC] $<<$ 1023 . Ein Vergleich der Parameter findet sich in Tabelle 2.2.

Tabelle 2.2: Standardwerte für EDCA Parameter von IEEE 802.11a [40].

AC	CWmin	CWmax	AIFSN	AIFS
AC_BK	15	1023	7	79 μs
AC_BE	15	1023	3	43 μs
AC_VI	7	15	2	34 μs
AC_VO	3	7	2	34 μs
WLAN DCF	15	1023	2	34 μs

2.3 Methoden der Leistungsbewertung

Um die Leistung von Ad-hoc-Netzen für den Katastrophenschutz bewerten zu können, werden drei Methoden eingesetzt. Im kleinen Maßstab werden Experimente durchgeführt, bei denen beispielsweise die erreichbare Datenrate, die bei einer Multi-Hop-Kommunikation erreicht werden kann, gemessen wird.

Sollen größere Szenarien untersucht werden, so wird eine Multiskalen-Simulation verwendet, die mehrere Simulationswerkzeuge miteinander verknüpft und hauptsächlich auf OMNeT++ basiert.

Für die Validierung einzelner Ergebnisse der Simulation wird ein analytisches Modell auf Basis von Markov-Ketten verwendet. Die mathematische Abbildung des zufallsbasierten Kanalzugriffs bei WLAN erlaubt die Berechnung der zu erwartenden Datenrate. Diese kann mit der in der Simulation gemessenen Datenrate verglichen werden.

2.3.1 Multiskalen-Simulation

Werden Kommunikationsnetze im Rahmen von Rettungseinsätzen und im Katastrophenschutz eingesetzt, so bestehen erhöhte Anforderungen an die Zuverlässigkeit. Um die Leistungsfähigkeit eines neuen Vernetzungskonzepts adäquat bewerten zu können, sind Werkzeuge notwendig, die ein möglichst genaues Modell bereitstellen. Die im Rahmen dieser Arbeit eingesetzte Multiskalen-Simulationsumgebung setzt dafür auf eine Kombination von *best-in-class*-Tools [48].

Aufgrund der besonderen Bedingungen, welche für Szenarien in diesem Bereich vorausgesetzt werden, reicht der klassische Ansatz einer Simulation nicht mehr aus. In diesem klassischen Ansatz werden alle Bereiche, welche nicht unbedingt den Kern des Untersuchungsschwerpunkts darstellen, entweder aus der Simulation ausgeblendet oder mit Hilfe einfachster Abschätzungen hinzugenommen. Für viele Simulationsszenarien mag dies eine akzeptable Lösung darstellen, nicht jedoch im

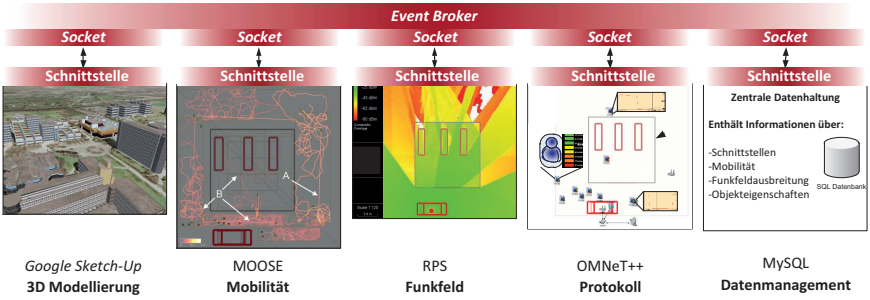


Abbildung 2.6: Multiskalen-Simulationsumgebung mit best-in-class-Tools

Bereich der Katastrophenszenarien. Insbesondere hier werden Umgebungsbedingungen angenommen, die nicht mit den Standard-Lösungsmethoden zu untersuchen sind. Es besteht auch nicht die Möglichkeit, eine Testumgebung zu nutzen, da die Bedingungen nur schwer in einem angemessenen Rahmen zu reproduzieren sind.

Die Multiskalen-Simulation bietet die Möglichkeit, Simulationen und Untersuchungen mit einem Detailgrad durchzuführen, welcher eine aussagekräftige Einschätzung über den Untersuchungsgegenstand zulässt. In Abbildung 2.6 sind die fünf Komponenten der Multiskalen-Simulation abgebildet. Bei der detaillierten Modellierung eines Szenarios für die Leistungsbewertung wird zunächst ein 3D-Modell mit Hilfe von *Google SketchUp* erstellt [11]. Dieses 3D-Modell dient als Grundlage für die Simulationsumgebung, insbesondere für die Funkfeldberechnung. Für diese wird der *Radio Propagation Simulator* (RPS) der Firma *radioplan* [16] eingesetzt, wobei RPS das 3D-Modell von *Google SketchUp* direkt importieren kann. Die Mobilität der Nutzer wird mit Hilfe von *MOOSE* [53] modelliert. Der Protokollsimulator OMNeT++ verknüpft die Tools mit seinem inhärenten *Event Broker* zu einer umfassenden Simulationsumgebung, wobei der Datenaustausch über eine zentrale Datenhaltung realisiert wird. Das MySQL Datenmanagement sorgt für eine schnellere Simulation. OMNeT++ kann aber auch direkt auf RPS zugreifen, was aber zu längeren Simulationsdauern führt.

Im Rahmen dieser Arbeit wird eine Multiskalen-Simulationsumgebung eingesetzt, welche innerhalb des Kontextes der Katastrophenszenarien eine Leistungsbewertung der eingesetzten WLAN-Netze und unterschiedlicher Routing-Protokolle ermöglicht. Dazu wurde ein 3D-Modell der Messe in Köln angefertigt, welches in RPS importiert wurde. Mit Hilfe von OMNeT++ wurde die WLAN-Kommunikation simuliert und eine umfassende Simulationsumgebung geschaffen.

2.3.2 Analytische Modellierung mit Markov-Ketten

Grundlagen der Markov-Modellierung

Ein Markov-Prozess ist zufallsbasiert, und der Wert einer Zufallsvariable hängt zum Zeitpunkt n nur von dem unmittelbar vorangegangenen Wert zum Zeitpunkt $n-1$ ab. In einem Markov-Prozess stellt die Zufallsvariable den Zustand eines Systems zu einem vorgegebenen Zeitpunkt n dar. Der Zustand eines Systems hängt von der Natur des zu untersuchenden Systems ab. Beispiele für solche Markov-Prozesse sind Telekommunikationsprotokolle.

Wenn der Zustandsraum eines Markov-Prozesses diskret ist, wird der Markov-Prozess als eine Markov-Kette bezeichnet [24], [89]. Bei der Analyse von MAC-Protokollen drahtloser Kommunikationsnetze, wie z.B. der DCF bei IEEE 802.11, wird von zeitdiskreten Markov-Ketten gesprochen [5]. In einem bestimmten Zustand einer Markov-Kette wird für eine gewisse Dauer, der so genannten "Wartezeit"(englisch *time slot*), gewartet. In einer zeitdiskreten Markov-Kette nimmt diese Wartezeit diskrete Werte an [5]. Das hat zur Folge, dass der Übergang von einem Zustand zum anderen bei diskreten Zeitwerten auftritt. Die Zeit t wird in diesem Fall bei bestimmten Zeitpunkten t_0, t_1, t_2, ... gemessen. Der Abstand zwischen den einzelnen Zeitschritten muss im Allgemeinen nicht gleich sein. Im Gegensatz dazu sind die diskreten Zeitwerte äquidistant [5], [6].

In einer zeitdiskreten Markov-Kette stellt der Wert der Zufallsvariablen (z.B. $S(n)$) den Zustand eines Systems zum Zeitpunkt n dar. Hierbei hängt die Zufallsvariable $S(n)$ nur von ihrem unmittelbar vorangegangenen Wert, d.h. nur von $S(n-1)$ ab. Dies wird als die Markov-Eigenschaft oder die gedächtnislose Eigenschaft (engl. *Markov property* oder *memoryless property*) einer Markov-Kette bezeichnet, wobei der aktuelle Zustand eines Systems nur von seinem unmittelbar vergangenen Zustand abhängt (vgl. [24] und [89]). Der Übergang von einem Zustand zum anderen wird nur durch eine sog. Übergangswahrscheinlichkeit bestimmt ohne Berücksichtigung, wie das System in den aktuellen Zustand gelangte.

Eine zeitdiskrete Markov-Kette ist im Gleichgewicht, wenn ihre Übergangswahrscheinlichkeiten nicht von den diskreten Zeitwerten n abhängig sind. In diesem Fall wird die Markov-Kette als homogen bezeichnet, und das System ist im stationären Zustand. Im stationären Zustand gelten folgende Gleichungen:

$$\sum_i s_i = 1$$

$$\sum_i p_{ij} s_i = \sum_j p_{ji} s_j$$

Dabei sind s_i bzw. s_j die Wahrscheinlichkeiten dafür, dass das System sich im Zustand i bzw. j befindet, und dass p_{ij} bzw. p_{ji} die Übergangswahrscheinlichkei-

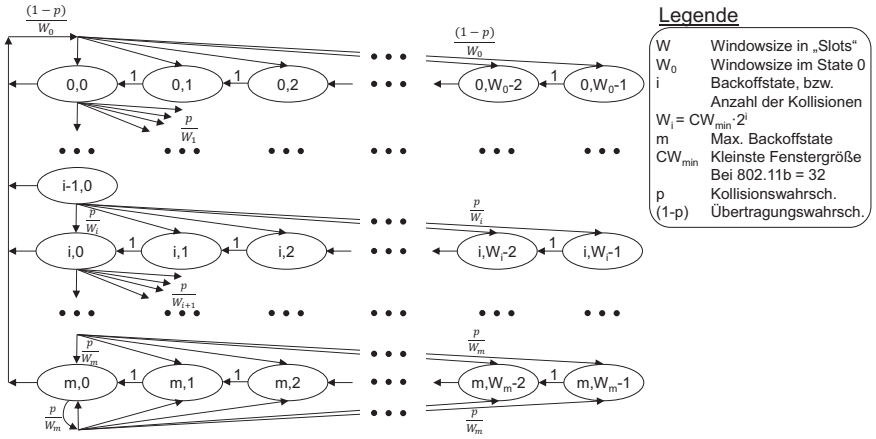


Abbildung 2.7: Zweidimensionale Markov-Kette der DCF (nach [5])

ten für den Übergang vom Zustand i zum Zustand j bzw. vom Zustand j zum Zustand i ist. Im stationären Zustand ist die Wahrscheinlichkeit zum Verlassen eines Zustands i gleich der Wahrscheinlichkeit für den Eintritt dieses Zustands.

Modellierung des Medienzugriffs bei WLAN

Der verteilte Medienzugriff bei WLAN basiert auf der *Distributed Coordination Function* (DCF). Die DCF kann durch eine Markov-Kette modelliert werden.

Im Rahmen dieser Arbeit wurde *Giuseppe Bianchi*, der Pionier der Markov-Modellierung der WLAN-DCF [5], per E-Mail kontaktiert [6], um die Annahmen für die Modellierung der DCF anhand von Markov-Ketten zu erfragen. Um die DCF anhand zeitdiskreter Markov-Ketten modellieren zu können, müssen demnach folgende Annahmen getroffen werden.

1. Für die zeitdiskrete Eigenschaft muss eine Zeitskalierung geschaffen werden. Der Prozess $b(t)$ im Bianchis Model, welcher den Backoff-Zähler eines Netzteilnehmers modelliert, sollte einen zeitdiskreten Prozess darstellen, wobei die diskreten Zeitwerte $t = 0, 1, 2, ...$ die Grenzen der *Time Slots* repräsentieren. Selbst wenn *Time Slots*, wie sie in [5] definiert werden, variable Größen haben, werden sie bei der im Bianchi-Model verwendeten Skalierung als einheitlich betrachtet.

2. Die zweite Annahme bezieht sich auf die Eigenschaft der Gedächtnislosigkeit. Da der Prozess $b(t)$ vom Verlauf der Übertragungen (z.B. von der Anzahl

der Wiederholungen einer Übertragung bei Kollisionen) eines Netzteilnehmers abhängt, gilt die gedächtnislose Eigenschaft für den Prozess $b(t)$ nicht. Dies wird aber überwunden, indem statt dem eindimensionalen Prozess $b(t)$ der zweidimensionalen Prozess $\{b(t), s(t)\}$ betrachtet wird, wobei $s(t)$ die i-te Wiederholung einer Übertragung darstellt. Es wird dann angenommen, dass jedes Paket bei jedem Versuch einer Übertragung und unabhängig von der Anzahl der schon wiederholten Übertragungen mit einer konstanten und unabhängigen Wahrscheinlichkeit p kollidiert. Somit entsteht eine zeitdiskrete Markov-Kette für den Prozess $\{b(t), s(t)\}$, da die Markov-Eigenschaft, nämlich die Abhängigkeit der Wahrscheinlichkeit des Übergangs vom aktuellen zum zukünftigen Zustand nur von der Wahrscheinlichkeit des aktuellen Zustands, für den Prozess $\{b(t), s(t)\}$ anwendbar ist. Die zweidimensionale Markov-Kette, die dieses Modell repräsentiert, ist in Abbildung 2.7 dargestellt.

Im Gegensatz zu [47] setzt *Bianchi* in seinem Modell eine sog. Überlastbedingung [5] (volle Auslastung des Systems) voraus, sodass bei jedem Netzteilnehmer die Sende-Warteschlange immer gefüllt ist.

2.3.3 Experimentelle Untersuchungen

Im Rahmen dieser Arbeit sind zahlreiche Experimente durchgeführt worden, um die Leistungsfähigkeit verschiedener Ad-hoc-Netze und der verwendeten Routing-Protokolle zu untersuchen. Dabei wurden hauptsächlich eingebettete Systeme eingesetzt, da sich deren Positionierung im Raum einfach verändern lässt. Es hätten anstatt von eingebetteten Systeme auch Laptops für die Experimente genutzt werden können. Der Vorteil von eingebetteten Systemen ist jedoch ihre geringe Größe, die auch ein Experiment im Freifeld mit hoher Knotenzahl erlaubt.

Tabelle 2.3: Eingesetzte Hardwareplattformen

	Dropped Unit	Laptop
System	Overo Gumstix	Lenovo T500
Architektur	ARM	x86
CPU	OMAP3503	Intel Core2Duo P8600
Taktung [MHz]	600	2400
RAM [MB]	512	8000
OS	Debian Linux	Ubuntu 12.04 LTS
Kernel	3.6.rc1	3.2.12

Für die Untersuchungen wurden zwei verschiedene eingebettete Systeme eingesetzt. Hauptsächlich wurden die Overo-Gumstix [27] verwendet, die im Rahmen

dieser Arbeit zu so genannten *Dropped Units* verbaut wurden. Diese auf der ARM-Architektur basierenden eingebetteten Systeme zeichnen sich aufgrund ihrer geringen Größe aus. Das System ist nur so groß wie ein Kaugummi-Streifen. Nähere Informationen zu den Gumstix sind im Kapitel 3.2.2 zu finden. Eine Übersicht zu den eingesetzten Hardwareplattformen ist in Tabelle 2.3 gegeben.

Für die meisten Untersuchungen wurde das Tool iPerf [41] verwendet, was neben der Datenrate auch die Verzögerung und den Jitter einer Verbindung misst.

3

Prozess-orientierte Ad-hoc-Vernetzung

In diesem Kapitel werden zunächst Dienste vorgestellt, welche von Rettungskräften im Katastrophenschutz eingesetzt werden können. Um diese Dienste nutzen zu können, wird ein Ad-hoc-Netz aufgebaut. Zur Ad-hoc-Vernetzung der Rettungskräfte werden Dropped Units als neuartige Hardware-Plattform für mobile WLAN-Router vorgeschlagen. Die Leistung der Dropped Units in Bezug auf die WLAN-Funkabdeckung wird mittels Simulation analysiert. Für den praktikablen Ausbringungsprozess der Dropped Units werden zwei Konzepte vorgestellt. Bei der audiovisuell unterstützten Platzierung (AVUP) werden Rettungskräfte beim Netzaufbau durch visuelle Indikatoren und Kontrolltöne bei der Auswahl eines geeigneten Standorts für einen WLAN-Router unterstützt. Das zweite Konzept sieht vor, dass der Netzaufbau in den Prozess der Rettungskräfte integriert wird. Beim Interkupplungskonzept werden die WLAN-Router in die Schlauchkupplungen von Feuerwehrschläuchen integriert, die eine standardisierte Länge aufweisen. Bei diesem Konzept folgt die Technik der Taktik, was den Endanwendern sehr wichtig ist.
Die in Abschnitt 3.4 dieses Kapitels beschriebenen Konzepte und Ergebnisse bauen auf Beiträgen des Autors zur Publikation [100] auf. Darüber hinaus bauen die Konzepte aus Abschnitt 3.6 dieses Kapitels auf Beiträgen des Autors zu den Publikationen [99] und [102] auf.

3.1 Szenarienspezifische Dienste

Bevor Lösungskonzepte für die Ad-hoc-Vernetzung der Rettungskräfte am Einsatzort vorgestellt werden, soll zunächst anhand von neuartigen Diensten der Grund für die Vernetzung verdeutlicht werden. Die neuen Dienste stellen einen Mehrwert für die Rettungskräfte dar und sind besonderes für den Einsatzleiter interessant.

Durch die nachfolgend vorgestellte digitale Lagekarte können Funksprüche vermieden werden, indem Rettungskräfte Gefahrensymbole mit ihrem Smartphone, oder ähnlichen IP fähigen Endgeräten, in die Lagekarte einfügen. Auch die anschließend vorgestellte Videoübertragung von Helmkameras unterstützt den Einsatzleiter bei der Bewertung einer Situation, um schnell auf Gefahren reagieren zu können.

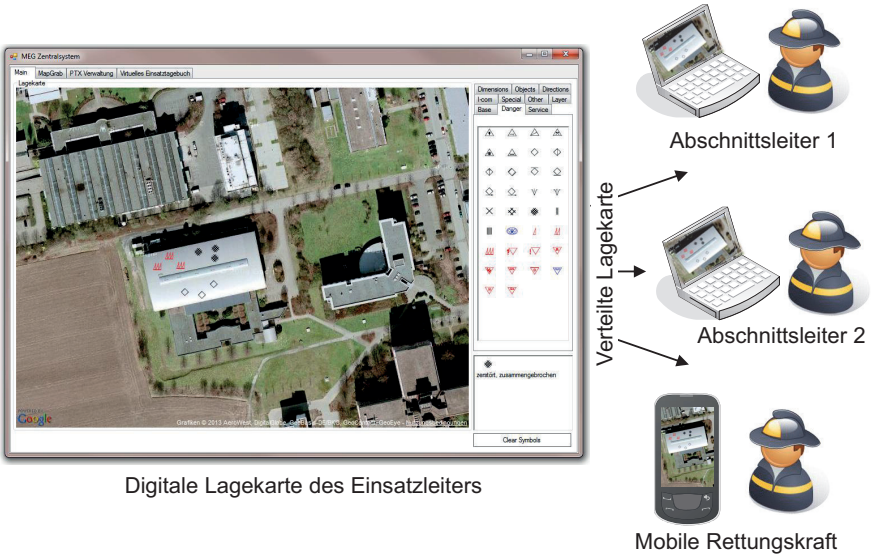


Abbildung 3.1: Digitale Lagekarte mit verteilter Darstellung

Diese Dienste haben unterschiedliche Anforderungen an das Kommunikationsnetz, insbesondere bezüglich Datenrate und Verzögerung. Nachfolgend werden beide Dienste vorgestellt, die im Rahmen dieser Arbeit im Kontext verschiedener Drittmittelprojekte entstanden sind.

3.1.1 Digitale Lagekarte

Der Dienst *Digitale Lagekarte* stellt im Vergleich zur Videoübertragung geringere Anforderungen an das Kommunikationsnetz. Die interaktive Lagekarte setzt jedoch die ständige Verfügbarkeit des Netzes voraus. Darüber hinaus soll der Dienst auf heterogenen Endgeräten funktionieren. Eine besondere Herausforderung stellt dabei die Vernetzung der Einsatzkräfte innerhalb von Gebäuden dar. Hier ist der Funkempfang oft durch die Außenwände stark gestört. In Abbildung 3.1 ist eine Lagekarte dargestellt, die im Rahmen dieser Arbeit im Projekt MobileEmerGIS (siehe Anhang A.1.4) entwickelt wurde. Die MobileEmerGIS-Symbole auf der digitalen Lagekarte entsprechen den taktischen Zeichen (vgl. Feuerwehr-Dienstvorschrift 100 [1]), die von den Rettungsorganisationen heutzutage auf Papier eingesetzt werden. Drei rote Dreiecke symbolisieren einen Vollbrand, die Raute symbolisiert eine Person und die gestrichelte Raute symbolisiert einen zerstörten Gebäudeteil. Die

Abbildung 3.2: Prototyp zur Videoübertragung von einer Helmkamera

Lagekarte wird dadurch interaktiv, dass neu eingezeichnete Symbole unverzüglich an alle Rettungskräfte und den Einsatzleiter verteilt werden.

Durch den Einsatz der digitalen Lagekarte können Funksprüche vermieden werden, die zurzeit noch genutzt werden, um dem Einsatzleiter und anderen Rettungskräften Gefahren mitzuteilen. Laut Aussagen des Bayerischen Roten Kreuzes stellt der Funkkanal eine beschränkte Ressource dar, welche die digitale Karte entlastet.

3.1.2 Videoübertragung von Helmkameras

Bei Gesprächen mit der Feuerwehr zur Anforderungsanalyse im Projekt SPIDER ist die Übertragung eines Live-Videos von den Helmkameras der Einsatzkräfte zum Einsatzleiter als sinnvolle Anwendung genannt worden. Diese Videoübertragung ist für das Kommunikationsnetz weitaus anspruchsvoller als die Übertragung von Sensorwerten und Positionsdaten für die digitale Lagekarte. Somit kann dieser Helmkamera-Dienst als Referenz betrachtet werden.

In Abbildung 3.2 ist die prototypische Realisierung der Videoübertragung dargestellt, die im Rahmen der hier vorliegenden Arbeit entstanden ist. Prinzipiell funktioniert die Videoübertragung wie folgt: Eine Rettungskraft, die mit einer Helmkamera ausgestattet ist, sieht ein Objekt. Das Bild dieses Objekts wird über WLAN an den Einsatzleiter gesendet, der anschließend dieses Bild auf seinem Monitor sehen kann.

In Abbildung 3.2 ist links eine Rettungskraft der Feuerwehr Gelsenkirchen mit Helm dargestellt. In diesen Helm wurde vorne eine Kamera integriert. Diese ist

(a) Prototyp (b) Labor Dropped Unit (c) Ultra-Mobile Dropped Unit

Abbildung 3.3: Evolution der Dropped Units

über USB an einen Embedded PC angeschlossen, der mittels WLAN mit einem Laptop kommunizieren kann. Auf dem Embedded PC wird ein Linux Betriebssystem ausgeführt. Zur Übertragung des Kamerabildes wird das Programm *MJPEG Streamer* [84] auf dem Embedded PC eingesetzt.

3.2 Neuartige Hardware-Plattform - Dropped Units

Da die existierenden Vernetzungskonzepte den Anforderungen der Feuerwehr in Bezug auf die Kosten und die Mobilität der Knoten nicht gerecht werden (siehe Kapitel 2.1.4), wird im Rahmen dieser Arbeit eine eigene Hardware-Plattform für die Vernetzung der Rettungskräfte am Einsatzort eingeführt. Diese Hardware-Plattform wird *Dropped Unit* genannt und erlaubt eine flexible, kostengünstige und mobile Konfiguration der Vernetzung.

Im Rahmen dieser Arbeit sind drei Varianten von *Dropped Units* entstanden. Der erste *Dropped Unit*-Prototyp nutzt das *Wireless Distribution System* (WDS). Da diese Plattform in Bezug auf das Routing relativ unflexibel ist, sind zwei weitere Prototypen entstanden, die beide auf einem eingebetteten System basieren, welches eine flexible Vernetzung durch anpassbare Routing-Protokolle ermöglicht. Diese beiden flexiblen Varianten der *Dropped Units* unterscheiden sich im Wesentlichen in Form und Größe.

3.2.1 Dropped Unit Prototyp - WLAN-Repeater

Die erste Version der *Dropped Unit* ist in Abbildung 3.3(a) dargestellt. Es wird eine Basishardware eingesetzt, die für die Vergrößerung eines WLAN-Empfangsbereichs das WDS-Verfahren einsetzt. Durch die relativ kleine Baugröße und ein Gewicht von nur 250g ist diese Basishardware als Ausgangsbasis für *Dropped Units* geeignet.

Die von der Feuerwehr gewünschte Flexibilität wird durch eine batteriebasierte Energieversorgung und ein Gehäuse mit kleiner Bauweise umgesetzt.

Im Laufe der Untersuchungen wurde festgestellt, dass das WDS relativ unflexibel und für den Aufbau von größeren mobilen Ad-hoc-Netzen eher ungeeignet ist. Daher wurde ein neuer Typ von *Dropped Units* gesucht, der auch die experimentelle Untersuchung von selbstkonfigurierenden Netzen unterstützt.

3.2.2 Eingebettetes System für flexible Vernetzung

Um unterschiedliche Routing-Protokolle experimentell evaluieren zu können, sind mehrere *Dropped Units* entstanden, die in Abbildung 3.3(b) dargestellt sind. Sie basieren auf einer Plattform, die eine flexible Konfiguration erlaubt. Darüber hinaus sollte die Plattform möglichst klein sein, damit sie mobil eingesetzt werden kann. Dabei fiel die Wahl auf das eingebettete System vom Typ *Overo* der Firma *Gumstix*. Dieses System ist mit einer ARM Cortex-A8 CPU bestückt und arbeitet mit einer Taktfrequenz von 600 MHz. Die Abmessungen des Gumstix betragen 80 mm x 40 mm x 7 mm. In diesen Maßen ist bereits das *Motherboard*, genannt *Summit*, eingeschlossen, auf welches der *Overo Embedded PC* eingesteckt wird und Schnittstellen wie beispielsweise USB bereitstellt.

Der Gumstix wird mit Linux betrieben, was den Vorteil hat, dass für Linux im Gegensatz zu Windows zahlreiche Routing-Protokolle verfügbar sind. Im Laufe der Arbeit wurde der Kernel immer aktuell gehalten und ist bei den letzten Experimenten bei Version 3.6.rc1 angekommen. Für den Gumstix wird ein spezieller Kernel aus dem Linux-OMAP-Zweig verwendet, der sich durch *Patches* für die OMAP CPU auszeichnet, die in den Hauptzweig der Kernel-Entwicklung nicht einfließen.

Der *Overo Gumstix* vom Typ *Fire* enthält bereits ab Werk ein WLAN-Modul. Es eignet sich jedoch nicht für den Betrieb im Ad-hoc-Modus, und es funkt nur im 2,4 GHz Band. Aufgrund dieser Einschränkungen wird an den Gumstix ein zusätzlicher WLAN-USB-Stick angeschlossen, der sowohl den Betrieb im 5 GHz Band als auch den Ad-hoc-Modus unterstützt. Auf dem Markt gibt es zahlreiche WLAN-Sticks, welche die Anforderungen erfüllen, aber nur wenige, die zusätzlich durch das Linux-Betriebssystem unterstützt werden. Aufgrund der Ergebnisse der Zusammenarbeit des WLAN-Chip-Herstellers Atheros mit der Linux-Community sind die Linux-Treiber für Atheros-Chipsätze zu den Evaluationszwecken, die im Rahmen dieser Arbeit durchgeführt werden, sehr gut geeignet.

Als WLAN-USB-Stick wird konkret der DWA-160 der Firma D-Link eingesetzt. Dieser USB-Stick erfüllt alle Anforderungen und erlaubt auch lange Einsatzzeiten, da er Lüftungsschlitze besitzt, die ein Überhitzen verhindern. In seinem Inneren kommt der Atheros-Chip AR9170 zum Einsatz, der IEEE 802.11 a/b/g/n unterstützt.

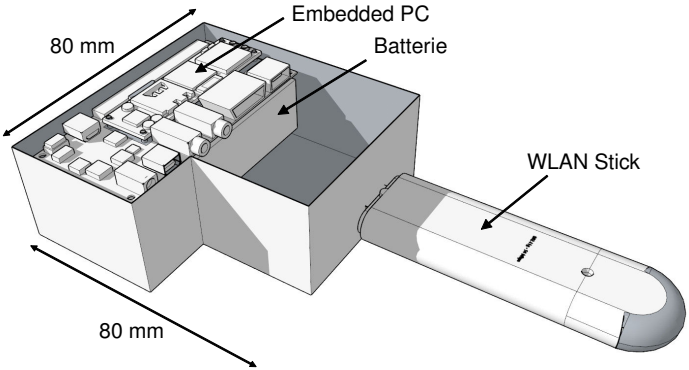


Abbildung 3.4: Ultra-Mobile Dropped Unit

Der Embedded PC wird mittels eines Lithium-Polymer-Akkumulators mit Energie versorgt. Es kommen Akkumulatoren vom Typ SLS EP 4400 mAh mit einer Nennspannung von 7,4 V zum Einsatz. Da der Embedded PC eine Eingangsspannung von 5 V benötigt, muss die Spannung des Akkus zunächst heruntergeregelt werden. Dazu wird ein *Switching Regulator* der Firma Dimension Engineering verwendet, der gegenüber einem Linearregler weniger thermische Verluste bei der Spannungswandlung aufweist.

Zum Schutz des Lipo-Akkus ist ein Lipo-Warner verbaut, der die *Dropped Unit* ausschaltet, wenn eine definierte Spannung unterschritten wird. Für den Einsatz im Labor ist eine alternative Spannungsversorgung mittels Labornetzteil vorgesehen.

3.2.3 Ultra-mobile Version der Dropped Units

Im Gespräch mit der Feuerwehr sind die *Labor Dropped Units* (siehe Abbildung 3.3(b)) als zu groß und zu schwer bezeichnet worden. Daher ist ein weiterer Prototyp entstanden, der den Anforderungen der Feuerwehr nach Form und Gewicht entspricht. In Abbildung 3.4 ist die ultra-mobile Version der *Dropped Units* dargestellt. Im Vergleich zur vorherigen Version wurde die Batterie ausgetauscht und auf den USB-Hub verzichtet. Durch den Einsatz einer so genannten Powerbank von *goobay*, welche normalerweise für die Aufladung eines Mobiltelefons unterwegs dient, kann auf den extra Spannungswandler verzichtet werden, da dieser bereits integriert ist. Die Powerbank hat eine Nennladung von 2000 mAh.

Das Gehäuse der ultra-mobilen *Dropped Unit* wurde passgenau für die Powerbank und den Gumstix entworfen und mit einer CNC-Fräse aus Epoxidharz-Platten

ausgeschnitten, was für eine sehr gute Stabilität sorgt. Zusätzlich konnten einige Kabel eingespart werden, was zusätzlich Platz und Gewicht eingespart hat. Bei einer Befragung zur Akzeptanz der ultra-mobilen *Dropped Unit* haben Mitarbeiter der Feuerwehr gesagt, dass die Größe und das Gewicht einsatztauglich seien.

3.2.4 Vertrauliche Kommunikation

Während Einsätzen von Rettungskräften bei Großschadenslagen werden sensible Daten übertragen. Ein Angreifer könnte abgehörte Informationen nutzen, um noch größeren Schaden anzurichten. Daher ist eine Verschlüsselung der Kommunikation von Rettungskräften notwendig. Erste Untersuchungen zur Verschlüsselung von IP-basierter Multimediakommunikation mittels einer Kombination von asymmetrischen und symmetrischen Verfahren stellte *Šubik* in [86] vor.

Ein gängiges Verfahren zum Verschlüsseln von WLAN Kommunikation ist aktuell WPA2. Dieses Verfahren wird auch von den *Dropped Units* verwendet, wobei sich hier eine Besonderheit ergibt. Die *Dropped Units* vernetzen sich untereinander im Ad-hoc-Modus. Die Verschlüsselung mit WPA2 im Ad-hoc-Modus funktioniert jedoch nicht ohne weiteres. Die in Laptops häufig verbauten Intel-Chipsätze unterstützen in der Regel die WPA2-Verschlüsselung in Kombination mit dem Ad-Hoc-Modus nicht. Im Rahmen der hier vorliegenden Arbeit wurden lediglich Chipsätze der Atheros als funktionstüchtig identifiziert.

Die Verschlüsselung im Ad-Hoc-Modus wird auf den *Dropped Units* mittels des Hilfsprogramms *wpa_supplicant* umgesetzt. Für die automatische Konfiguration wurden Linux-Skripte geschrieben, die anhand der MAC-Adresse des eingesteckten WLAN-USB-Sticks die Verschlüsselung und das Ad-Hoc-Netz auswählen.

Für zukünftige Projekte wird vorgeschlagen, nicht mehr WPA2, sondern ein sicheres Routing-Protokoll einzusetzen. Im Rahmen des Projekts SPIDER haben *Sbeiti et al.* das Protokoll *Position Aware Secure and Efficient Route Discovery*, kurz PASER, entwickelt [71], [70]. PASER nutzt als Basis ein unverschlüsseltes Ad-hoc-Netz und unterscheidet zwischen vertraulichen und nicht-vertraulichen Knoten. Möchte ein Knoten an der Kommunikation teilnehmen, so muss er sich erst mit einem Zertifikat bei der Zertifizierungsstelle authentifizieren. Sobald dem Knoten vertraut wird, kann er an der verschlüsselten Kommunikation teilnehmen. Der Einsatz von PASER hat den Vorteil, dass mehr Chipsätze für die Ad-hoc-Vernetzung genutzt werden können, und dass im Falle einer Kompromittierung der Verschlüsselung flexibler reagiert werden kann. Falls die Verschlüsselung von WPA2 von Angreifern umgangen würde, müsste möglicherweise die WLAN Hardware ausgetauscht werden.

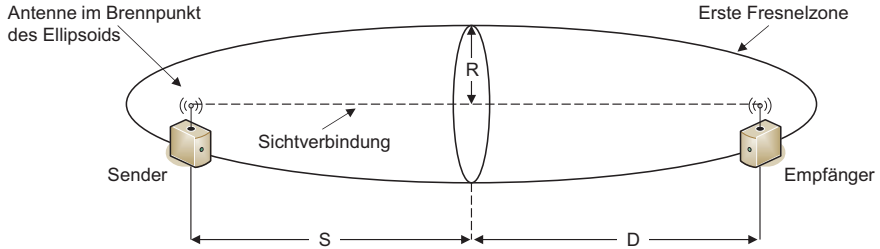


Abbildung 3.5: Erste Fresnelzone zwischen Sende- und Empfangsantenne

3.3 Einfluss der Antennenhöhe auf die Kommunikation

Der Name *Dropped Unit* erweckt den Anschein, als ob WLAN-Knoten direkt auf den Boden abgelegt werden würden. Aufgrund der Funkausbreitungseigenschaften von WLAN ist eine Platzierung der Kommunikationsantenne auf Bodenhöhe jedoch unvorteilhaft. Im Einsatz müsste die Antenne der *Dropped Units* daher auf einem Stativ montiert werden, oder über eine ausziehbare Antenne auf eine praktikable Höhe gebracht werden. Die Frage in welcher Höhe sich die Antenne über dem Boden befinden müsste, wurde zunächst analytisch untersucht und anschließend in einem Experiment validiert.

3.3.1 Analytische Untersuchung des Einflusses der Antennenhöhe mittels Betrachtung der Fresnelzone

Die Funkübertragung zwischen Sende- und Empfangsantenne kann durch Hindernisse gestört werden, die sich nicht in der direkten Sichtverbindung zwischen beiden Antennen befinden. Dies liegt an dem Wellencharakter des Funksignals. Ein nützliches Konzept zur Überprüfung, ob die Übertragung durch Hindernisse gestört wird, ist die erste Fresnelzone [78] [82] [23]. Es gibt mehrere Fresnelzonen, wobei jedoch nur die Erste praxisrelevant ist. In Abbildung 3.5 ist die erste Fresnelzone zwischen einem Sender und einem Empfänger schematisch dargestellt. Sie hat die Form eines Rotationsellipsoids, wobei sich die Antennen in den Brennpunkten des Ellipsoids befinden. Der Radius in Metern des Ellipsoids zwischen Sender und Empfänger lässt sich mit der Formel 3.1 berechnen (nach [82]).

$$R_m = 17{,}3\sqrt{\frac{S_{km} \cdot D_{km}}{f_{GHz} \cdot (S_{km} + D_{km})}} \tag{3.1}$$

Für den maximalen Radius R_{max}, der sich genau zwischen Sender und Empfänger befindet, lässt sich die Formel mit $S_{km} = D_{km}$ wie folgt vereinfachen.

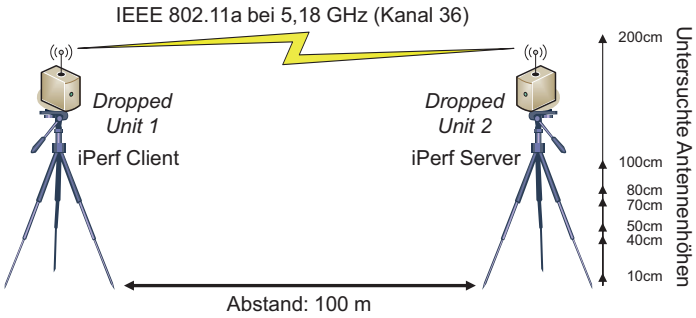


Abbildung 3.6: Schematische Darstellung des Versuchsaufbaus

$$R_{max} = 8,65\sqrt{\frac{Dist_{km}}{f_{GHz}}} \tag{3.2}$$

Freeman spricht in [23] davon, dass es in der Praxis ausreicht, 60% der ersten Fresnelzone frei von Hindernissen zu halten, um die Übertragung zwischen den beiden Antennen nicht zu beeinflussen. *Stallings* weist in [82] darauf hin, dass in diesem Zusammenhang insbesondere der Boden von Bedeutung ist und daher Sende- und Empfangsantenne mindestens $0,6 \cdot R_{max}$ über dem Boden platziert werden müssen.

Dieser Zusammenhang wird im Folgenden experimentell untersucht. Sende- und Empfangsantenne werden in 100 m Abstand voneinander aufgestellt und die Übertragung findet bei 5,18 GHz statt. Damit ergibt sich für 60% von R_{max}:

$$0,6 \cdot R_{max} = 0,6 \cdot 8,65\sqrt{\frac{0,1}{5,18}} \approx 0,72m \tag{3.3}$$

Somit müssen die beiden Antennen in ca. 72 cm Höhe platziert werden, damit bei der Signalübertragung die Dämpfung durch den Boden näherungsweise vernachlässigt werden kann.

3.3.2 Versuchsaufbau zum Einfluss unterschiedlicher Antennenhöhen auf die Datenrate

Der Versuchsaufbau zur experimentellen Untersuchung des Einflusses der Antennenhöhe auf die Datenrate einer WLAN Kommunikation ist in Abbildung 3.6 dargestellt. Es wurden zwei *Dropped Units* im Abstand von 100 m voneinander positioniert, wobei sie jeweils auf ein höhenverstellbares Stativ montiert waren.

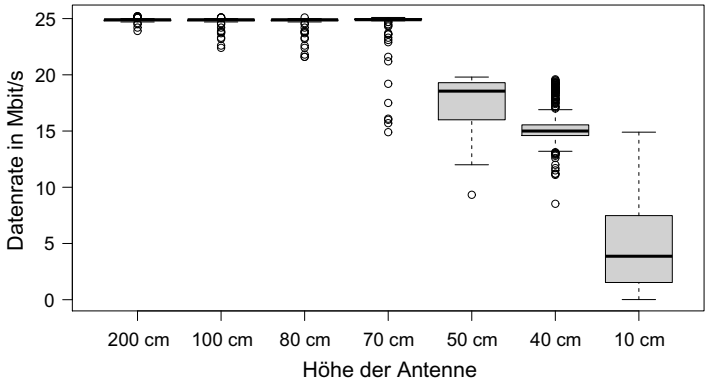


Abbildung 3.7: Experimentelles Ergebnis der Abhängigkeit der Datenrate von der Antennenhöhe bei 100 m Antennenabstand

Die beiden *Units* kommunizierten im WLAN-Ad-hoc-Modus miteinander, wobei der Kanal 36 (5,18 GHz) nach IEEE 802.11a eingesetzt wurde. Auf der *Dropped Unit* 1 wurde ein iPerf Client und auf *Dropped Unit* 2 ein iPerf Server gestartet. Mittels iPerf konnte die erreichbare Datenrate in Abhängigkeit der Höhe gemessen werden. Die jeweils drei Minuten dauernde Messung wurde für sieben unterschiedliche Höhen durchgeführt und für jede Höhe im Abstand weniger Minuten zwei Mal wiederholt. Es wurden die Standardparameter für iPerf verwendet, wobei der UDP Modus mit einer Eingangsdatenrate von 30 Mbit/s gewählt wurde. Für das Experiment wurde die Datenrate am Empfänger (iPerf Server) jede Sekunde ausgegeben und protokolliert, wobei die protokollierte Datenrate in einer Sekunde einem Messpunkt entspricht.

3.3.3 Ergebnisse der Untersuchung

Die Ergebnisse der Untersuchung sind in Abbildung 3.7 als Boxplot-Diagramm dargestellt. Jeder Boxplot besteht aus zwei mal 180 Messpunkten. Auf der X-Achse der Abbildung ist die Antennenhöhe und auf der Y-Achse die in iPerf erreichte Datenrate aufgetragen. Für Antennenhöhen über 70 cm wird bis auf wenige Ausreißer eine Datenrate von ca. 25 Mbit/s erreicht, was der maximal erreichbaren Datenrate der eingesetzten Hardware entspricht. Bei niedrigeren Antennenhöhen nimmt die Datenrate ab. Werden die beiden *Dropped Units* auf den Boden gestellt, befindet sich die Antenne in 10 cm Höhe. Im Mittel wird dann nur noch eine Datenrate von ca. 4 Mbit/s erreicht. Bei dieser Messung ist im Gegensatz zu allen anderen Höhen die Verbindung jedoch ständig unterbrochen worden, was dazu führt, dass das Ergebnis für die 10 cm Messung eigentlich noch schlechter ausfällt.

3.3.4 Konsequenz der Untersuchung

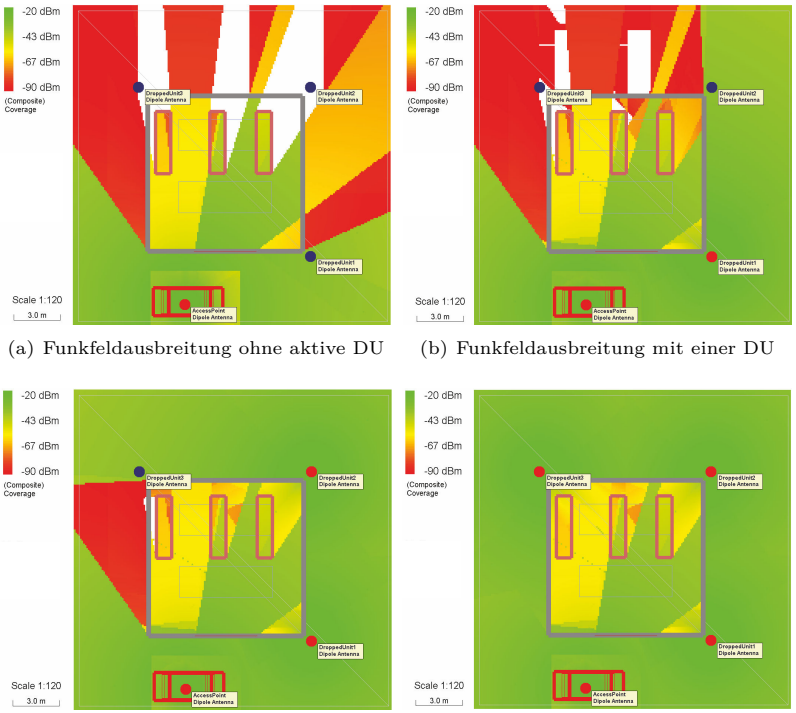
Die oben beschriebenen Ergebnisse zeigen, dass die Datenrate bis zu einer bestimmten Mindesthöhe von der Antennenhöhe abhängt. Wenn Sender und Empfänger 100 m voneinander entfernt aufgestellt werden, dann beträgt diese Mindesthöhe ca. 70 cm. Diese Mindesthöhe stimmt auch gut mit der in Formel 3.3 analytisch bestimmten 60%igen Höhe der Fresnelzone überein ($0,6 \cdot R_{max} \approx 72cm$). Unterhalb der Mindesthöhe sinkt die Datenrate ab. Daher sollten die *Dropped Units* immer mindestens so hoch aufgestellt werden, dass die Mindesthöhe erreicht wird. Im Folgenden wird durch vielfältige Maßnahmen sichergestellt, dass die Mindesthöhe für die Antennenhöhe eingehalten wird. In der Praxis könnte die Mindesthöhe z.B. durch den Einsatz von Stativen, durch Befestigung an Laternenmasten oder durch das Platzieren auf Fensterbänken sichergestellt werden. Das Platzieren auf dem Boden würde ohnehin kaum in Frage kommen, da Rettungskräfte über eine Abgelegte *Dropped Unit* stolpern könnten.

3.4 Abdeckungsanalyse des Konzepts mittels Simulation

Die Leistungsfähigkeit der Vernetzung mittels der *Dropped Units* in Bezug auf die Anforderung nach einer lückenlosen Abdeckung wird mittels der Multiskalen-Simulationsumgebung untersucht. Es wird zunächst ein kleines Szenario untersucht. Das Szenario besteht aus einer 10 m · 10 m großen Halle, einem Fahrzeug mit installiertem WLAN Access Point und zehn Rettungskräften. Eine spezielle Rettungskraft, der zirkuläre Erkunder, umrundet zu Beginn des Einsatzes die Halle. Anschließend bewegt er sich, wie die anderen Rettungskräfte, zufällig (*random walk*) in der Nähe des Halleneingangs. Der Einsatz hat eine Dauer von einer Stunde.

In Abbildung 3.8(a) ist die Funkausbreitung des WLAN Access Points zu Beginn des Einsatzes gezeigt. Die Analyse wurde mit dem Radio Propagation Simulator der Firma Radioplan durchgeführt. Es ist zu sehen, dass der vordere Bereich der Halle, vor dem das Einsatzfahrzeug parkt, gut mit WLAN abgedeckt wird (grüner Bereich). Aufgrund eines geöffneten Hallentors ist auch der Innenbereich ausreichend abgedeckt. An den Außenseiten der Halle ist das Signal für eine Kommunikation zu schwach (orangener Bereich). Die Rückseite der Halle wird kaum abgedeckt (weiße Bereiche). Werden von dem Erkunder beim Umrunden der Halle *Dropped Units* abgelegt, so verbessert sich die Abdeckung bis zur lückenlosen Abdeckung in Abbildung 3.8(d) bei Verwendung von drei *Dropped Units*.

Das Szenario wird mit Hilfe von OMNeT++ untersucht. Die Simulationsumgebung ist in Abbildung 3.9 dargestellt. Zu sehen sind zwei kleine Programm-Fenster und ein Szenarienfenster im Hintergrund. Das Szenarienfenster zeigt eine 2D-Karte des Szenarios, ähnlich zu der Abdeckungsanalyse aus Abbildung 3.8.



(a) Funkfeldausbreitung ohne aktive DU

(b) Funkfeldausbreitung mit einer DU

(c) Funkfeldausbreitung mit zwei DUs

(d) Funkfeldausbreitung mit drei DUs

Abbildung 3.8: Abdeckungsanalyse der Funkfeldausbreitung für WLAN im Beispielszenario mit unterschiedlicher Anzahl von aktiven Dropped Units (DU)

Im kleinen Fenster unten links ist der qualitative Verlauf der Signalstärke über die Zeit des zirkulären Erkunders dargestellt. Der Erkunder platziert immer dann eine *Dropped Unit*, wenn die Signalstärke einen voreingestellten Pegel unterschreitet. Nach dem Deponieren der *Dropped Unit* steigt die Signalstärke umgehend an, was sich am Verlauf der Signalstärke zeigt. Im Szenarienfenster sind neben dem Erkunder noch weitere Rettungskräfte zu sehen. Diese befinden sich hauptsächlich in der Nähe des Einsatzfahrzeugs. Eine Rettungskraft befindet sich innerhalb der Halle.

Das kleine Programmfenster oben rechts zeigt die Pfade des Mobilitätsmodells. Dabei wird zwischen dem Pfad des zirkulären Erkunders und den anderen Rettungskräften unterschieden. Für die Simulation der Mobilität wurde *MOOSE* eingesetzt [53].

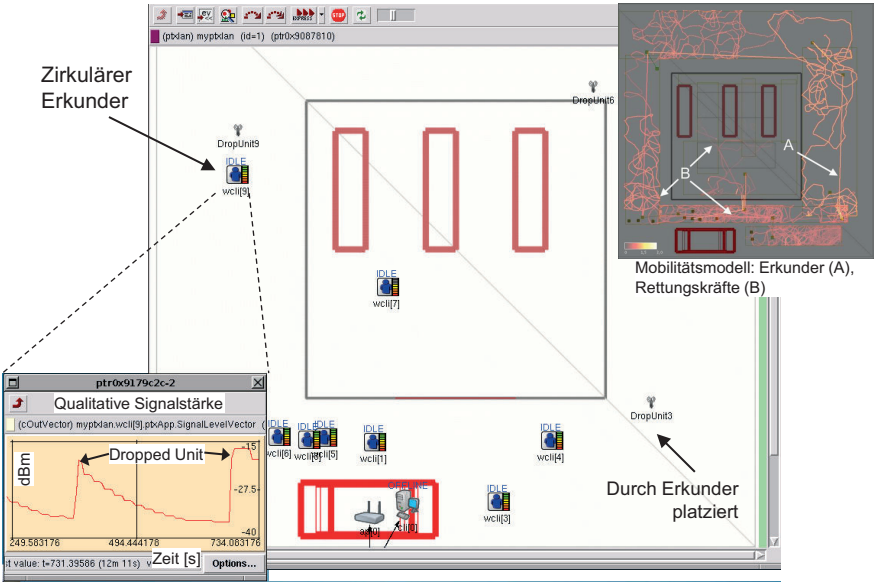


Abbildung 3.9: Simulation des Szenarios in OMNeT

Der Erkunder hat auf seinem Weg um die Halle herum drei *Dropped Units* platziert. Damit ist das Szenario mit WLAN abgedeckt. Nach seiner Umrundung begibt sich der Erkunder auch in den vorderen Bereich der Halle und bewegt sich hier zufällig mittels *random walk*. Die Einsatzdauer beträgt eine Stunde.

Leistungsbewertung

Mittels der Simulation soll im Folgenden untersucht werden, wie viele *Dropped Units* benötigt werden, um ein Kommunikationsnetz mit einer lückenlosen Abdeckung aufzubauen. Ziel ist es, eine Verfügbarkeit des Netzes für die mobilen Rettungskräfte von 100% während der Einsatzdauer zu erreichen. Dies ist gleichbedeutend mit der Forderung, dass eine Rettungskraft zu keiner Zeit des Einsatzes offline sein darf, also ohne Verbindung zum Einsatzleiter.

Zu jedem Szenario wurden 10 Simulationsdurchläufe ausgeführt. Bei jedem Durchlauf haben sich die simulierten Rettungskräfte auf anderen Pfaden mittels *random walk* bewegt.

Nachfolgend werden die Simulationsergebnisse zu zwei Rettungskräften exemplarisch untersucht. In Abbildung 3.10 ist das Ergebnis des zirkulären Erkunders

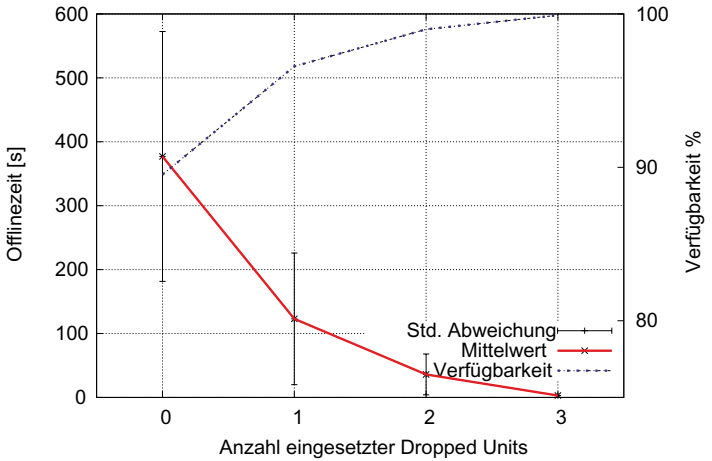


Abbildung 3.10: Offlinezeit und Verfügbarkeit des zirkulären Erkunders in Bezug zu eingesetzten Dropped Units (10 Sim. Durchläufe)

dargestellt. Auf der x-Achse ist die Anzahl der im Szenario platzierten *Dropped Units* dargestellt und auf y-Achse ist in Blau die Offlinezeit in Sekunden und zusätzlich in Rot die Verfügbarkeit in % aufgetragen. Es wurden 10 Simulationen mit unterschiedlichen Bewegungsmustern der Rettungskräfte durchgeführt. Dies führt dazu, dass die Offlinezeit ohne den Einsatz einer *Dropped Unit* in einem Bereich von ca. 180 s bis 580 s liegt. Im Mittel beträgt die Offlinezeit ohne *Dropped Unit* ca. 380 s. Bezogen auf die Einsatzdauer von einer Stunde (3600 s) ergibt sich somit ohne Einsatz von *Dropped Units* im Mittel eine Verfügbarkeit von 90%.

Dieses Ergebnis ist damit zu erklären, dass der Erkunder zu Beginn des Einsatzes um die Halle herum läuft. Anschließend bewegt er sich vor der Halle in der Nähe des Einsatzleitwagens. Da bei jedem Simulationsdurchlauf ein anderer Pfad gewählt wird, ist die Standardabweichung der Offlinezeit ca. 200 s groß. Eine Komponente der Offlinezeit, die ca. 180 s dauert, kommt durch die Umrundung der Halle zustande, weil an der West-, Ost- und Nordseite der Halle keine WLAN-Kommunikation möglich ist. Der Rest der Offlinezeit kommt durch den zufälligen Aufenthalt der Rettungskraft in nicht abgedeckten Bereichen zustande.

Wirft der Erkunder eine *Dropped Unit* ab, so verringert sich die Offlinezeit auf ca. 20 s bis 220 s, im Mittel auf 120 s. Durch den Abwurf an der Ostseite der Halle ist dieser Bereich mit WLAN abgedeckt. Je nach Laufgeschwindigkeit beim Umrunden und dem anschließend zurückgelegten Weg kommt es nun zu Offlinezeiten auf der Nord- und Westseite. Mit Bezug auf die Einsatzzeit erreicht die Verfügbarkeit des Erkunders bei Verwendung von einer *Dropped Unit* im Mittel 97%.

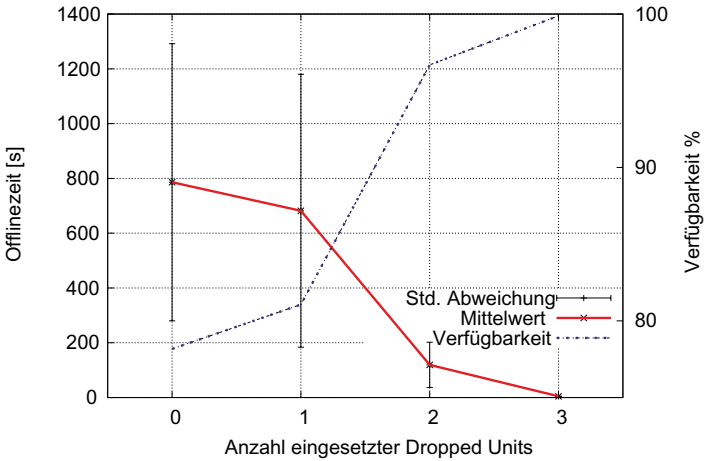


Abbildung 3.11: Offlinezeit und Verfügbarkeit eines Truppmanns des westlichen Angriffstrupps in Abhängigkeit von eingesetzten *Dropped Units* (10 Sim. Durchläufe)

Der Abwurf einer weiteren *Dropped Unit* auf der Nordseite der Halle führt zu einer weiteren Verkürzung der Offlinezeit. Diese reicht bei Verwendung von zwei *Dropped Units* von wenigen Sekunden, die der Erkunder zum Abschreiten der Westseite braucht, bis zu 80 Sekunden, wenn der Erkunder sich im späteren Einsatzverlauf nochmal auf der Westseite der Halle bewegt. Im Schnitt erreicht er eine Verfügbarkeit von ca. 99%.

Mit Abwurf der dritten *Dropped Unit* auf der Westseite der Halle ist eine komplette WLAN-Abdeckung des Szenarios erreicht. Die Offlinezeit sinkt auf 0 s, und somit ist die Anforderung an die Verfügbarkeit von 100% während der Einsatzdauer bei Verwendung von drei *Dropped Units* erfüllt.

In Abbildung 3.11 ist das Simulationsergebnis des westlichen Angriffstruppführers dargestellt. Das Bewegungsmuster dieser Rettungskraft unterscheidet sich deutlich von der Bewegung des Erkunders. Der westliche Angriffstrupp bewegt sich während des Einsatzes häufig auf der Westseite der Halle. In der Simulation wird ihm ein rechteckiger Bereich auf der Westseite der Halle zugewiesen, der bis an den südlichen Rand des Szenarios reicht. Da der Truppführer eine zufällige Standortänderung (*random walk* [81]) innerhalb dieses Bereichs ausführt ist die Spanne der Offlinezeit ohne Verwendung einer *Dropped Unit* sehr groß. Diese reicht von ca. 300 s bis ca. 1300 s und liegt im Durschnitt bei 800 s. Dies entspricht einer Verfügbarkeit von ca. 77%.

Wird vom zirkulären Erkunder eine *Dropped Unit* auf der Ostseite der Halle abgeworfen, so hat dies auf die Offlinezeit des Angriffstruppführers auf der Westseite nur geringe Auswirkungen. Die Spanne der Ausfallzeit bleibt ungefähr gleich lang, nur der Mittelwert verschiebt sich um ca. 100 s auf ca. 700 s Offlinezeit.

Erst der Abwurf einer zweiten *Dropped Unit* auf der Nordseite der Halle durch den Erkunder führt zu einer deutlichen Verbesserung der Offlinezeit. Nun ist auf der Westseite der Halle nur noch ein kleiner Bereich nicht mit WLAN versorgt. Während des Einsatzdauer kommt es bei dem westlichen Angriffstruppführer nur noch zu Offlinezeiten zwischen 20 s und 200 s. Im Mittel liegt die Verfügbarkeit bei 97%.

Wirft der Erkunder auch auf der Westseite eine *Dropped Unit* ab, dann sinkt die Offlinezeit auf 0 s und erreicht damit eine Verfügbarkeit von 100%. Es kommt zu keinem Ausfall mehr, da angenommen wird, dass der Angriffstrupp sich erst auf die Westseite der Halle zubewegt, wenn der Erkunder von seinem Rundlauf zurückkehrt.

Aus den Ergebnissen können einfache Regeln abgeleitet werden: *Dropped Units* sollten vornehmlich an Gebäudeecken und in Durchgängen platziert werden, da hinter Gebäudeecken mit WLAN-Abbrüchen zu rechnen ist.

Die hier vorgestellten Ergebnisse bezüglich der Offlinezeit und Verfügbarkeit aus Abbildungen 3.10 und 3.11 wurden in [100] veröffentlicht.

3.5 Audiovisuell unterstützte Platzierung - AVUP

Als erste einfache Lösung zur anwendergerechten, prozess-orientierten Ausbringung der *Dropped Units* wird die audiovisuell unterstützte Platzierung (AVUP) vorgeschlagen. Der Lösungsansatz wird nachfolgend anhand eines einfachen Szenarios erläutert. In Abbildung 3.12 ist exemplarisch ein Szenario mit drei Rettungskräften dargestellt. Die Rettungskräfte sind mit visuellen Signalgebern ausgestattet, welche die Signalstärke zu einem Access Point (AP) am Einsatzleitwagen in den drei Qualitätsstufen rot, gelb und grün anzeigen. Der Signalgeber ist hier in Form einer Ampel gegeben. Befindet sich die Rettungskraft in der Nähe des AP, so ist die Signalstärke gut (Ampel grün). Am Rand des Abdeckungsbereichs wird das Signal schwächer (Ampel gelb). Außerhalb des WLAN-Abdeckungsbereichs wird kein Signal mehr empfangen (Ampel rot). Zusätzlich zu der visuellen Komponente kann ein akustisches Signal ausgegeben werden, damit die Rettungskraft nicht ständig auf den visuellen Signalgeber schauen muss. Der akustische Signalgeber kann ähnliche Geräusche erzeugen wie die akustische Einparkhilfe bei modernen PKWs. Ist die Ampel grün, so wird nur selten ein Ton abgegeben. Je schwächer das Empfangssignal wird, desto häufiger wird der Ton zu hören sein. Außerhalb des Abdeckungsbereiches wird der Ton permanent erklingen.

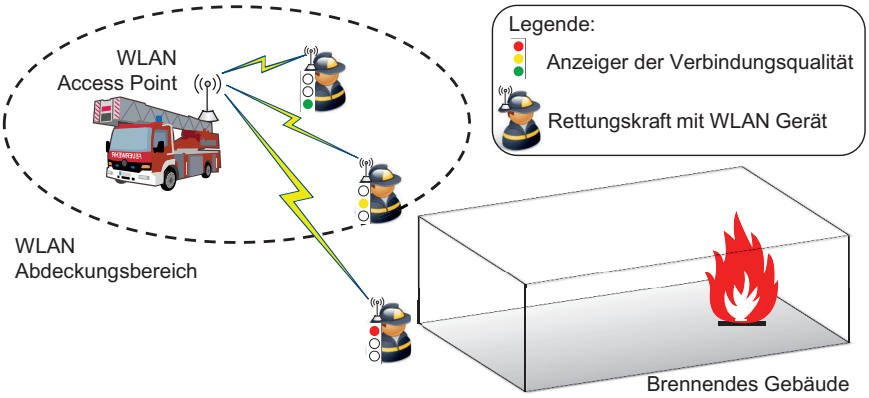


Abbildung 3.12: WLAN-Abdeckung durch einzelnen Access Point unzureichend

Damit Rettungskräfte auch innerhalb von Gebäuden, welche typischerweise außerhalb des WLAN-Abdeckungsbereiches eines vor dem Gebäude platzierten Access Point liegen, mit der Besatzung eines Einsatzfahrzeug in Kontakt bleiben können, sollen batteriebetriebene WLAN-Router am Rand des Abdeckungsbereiches platziert werden. Die Platzierung einer *Dropped Unit* kann dann erfolgen, wenn die Rettungskraft eine schnelle Tonfolge hört und die Ampel gelb anzeigt. Das Konzept kann von allen Rettungsorganisationen eingesetzt werden, wobei nachfolgend exemplarisch der Einsatz bei der Feuerwehr untersucht wird. Wird die Feuerwehr zu einem Einsatz gerufen, so rückt in der Regel ein sogenannter Zug aus. Teil dieses Fahrzeugverbands ist der Einsatzleitwagen (ELW). Es wird angenommen, dass ein WLAN Access Point auf dem ELW installiert ist. Der ELW ist mit dem Einsatzleiter besetzt, der von den Rettungskräften Rückmeldungen, i.a. in Form von Helmkameravideos, erhält und an die Rettungskräfte Befehle erteilt.

Es wird angenommen, dass ein Feuerwehrmann aus dem Zug den Einsatzort zu Beginn des Einsatzes erkundet. Dieser zirkuläre Erkunder umrundet das Gefahrengebiet und wirft dabei *Dropped Units* ab, wenn er den Rand des WLAN-Empfangsgebietes erreicht. Als Indikator zum Abwurf dient dabei die oben beschriebene Signalstärkenanzeige (siehe Ampel in Abbildung 3.13). Nach der Rückkehr des Erkunders zum ELW ist der Außenbereich des Einsatzortes mit WLAN abgedeckt.

In dem hier untersuchten Szenario wird eine rein lokale Kommunikation betrachtet. Es sind jedoch auch Szenarien denkbar, bei denen eine Kommunikationsverbindung zwischen dem Kommunikationsnetz der Rettungskräfte vor Ort und dem Hauptquartier der Rettungskräfte in einiger Entfernung benötigt wird. Da im Katastrophenfall davon ausgegangen wird, dass eine möglicherweise vorhande-

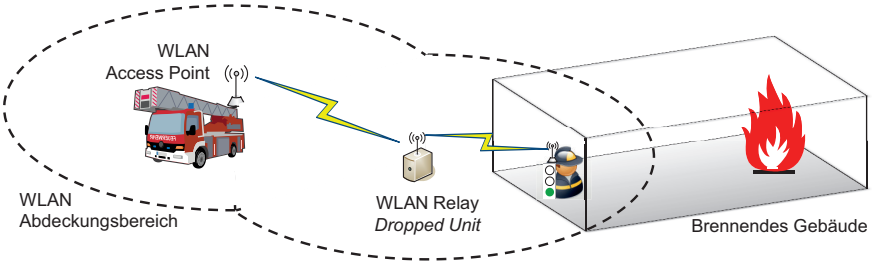


Abbildung 3.13: WLAN Abdeckung durch *Dropped Unit* erweitert

ne Kommunikationsinfrastruktur defekt ist, muss die Kommunikation über einen unabhängigen Kommunikationskanal erfolgen. *Hadhrami et al.* stellen in [28] UrgentMesh vor, bei dem das Mesh-Netz vor Ort mittels DVB-S2 mit dem Hauptquartier verbunden wird. Einen ähnlichen Ansatz verfolgt auch *Niehöfer* in [59]. Dieser Ansatz ist im Rahmen des Projekts SPIDER entstanden und schlägt ein rechenzeitoptimierendes Verfahren zur Berechnung der optimalen Positionierung des Einsatzleitwagens am Einsatzort vor, damit an der Parkposition die Kommunikation mittels DVB-S2 zuverlässig funktioniert.

3.6 Prozessorientiertes Platzieren von Routern

Die audiovisuell unterstützte Platzierung von WLAN-Routern kann die Rettungskräfte in manchen Situationen von ihrer eigentlichen Aufgabe abhalten. Auch der enorme Zeitdruck verhindert das adäquate Positionieren von *Dropped Units*. Daher wurde im Gespräch mit der Feuerwehr Gelsenkirchen nach neuen Konzepten für die prozess-integrierte Routerplatzierung gesucht. Als besserer Ansatz wurde von Seiten der Anwender eine prozessorientierte Platzierung der *Dropped Units* durch Integration der Hardware in das Rettungsequipment empfunden. Integriert werden könnte die Hardware in folgendes Equipment (siehe Abbildung 3.14):

- Schlauchtragekörbe
- Schlauchkupplungen
- Drehleiterwagen
- Einsatzfahrzeuge

Da auch schwer zugängliche Orte, wie z.B. Keller oder Tunnel, bei Großschadenslagen mittels WLAN abgedeckt werden sollen, sind Drehleiterwagen und Einsatzfahrzeuge für die Integration der *Dropped Units* allein nicht ausreichend. Der Drehleiterwagen kann jedoch durch eine am ausgefahren Rettungskorb befestigte

Abbildung 3.14: Rettungsequipment für mögliche Integration der *Dropped Units*

Dropped Unit eine sehr gute Außenabdeckung erzielen. Schlauchtragekörbe werden häufig bis zum Eingang eines gefährdeten Raumes mitgetragen und dann dort zurückgelassen. Es ist im Allgemeinen unsicher, ob die bei der Großsschadenslage abgelegten Schlauchtragekörbe eine ausreichende WLAN Abdeckung erzeugen würden, wenn sie mit *Dropped Units* ausgestattet wären. Die Integration der *Dropped Units* in die Schlauchkupplungen führt jedoch im Allgemeinen dazu, dass regelmäßig eine *Dropped Unit* platziert wird und somit von einer hinreichenden WLAN Abdeckung ausgegangen werden kann.

Um ein Feuer zu löschen, verlegen Feuerwehrleute einen Schlauch vom Löschfahrzeug zum Feuer. Der Schlauch besteht in Deutschland aus mehreren einzelnen Schlauchstücken. Für die hier vorgestellte Untersuchung wird eine Schlauchlänge von 20 Metern gewählt, welches die Standardlänge für Schläuche der Größe B in Deutschland ist [18]. Somit besteht der Gesamtschlauch aus mehreren 20m-Stücken. Jedes dieser 20m-Schlauchstücke wird mittels Kupplungen miteinander verknüpft.

Die in die Schlauchkupplungen integrieren *Dropped Units* werden nachfolgend *Inter-Coupling Unit* oder *InCo Unit* genannt. Der Name ist angelehnt an die zuvor eingeführten *Dropped Units*, da beide *Units* auf der gleichen Hardware beruhen.

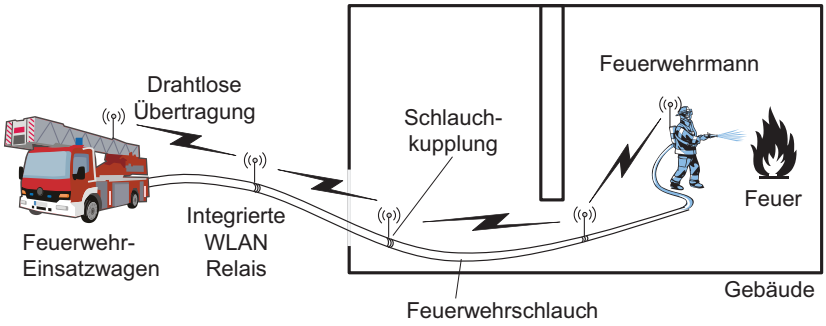


Abbildung 3.15: Prozesskonformer Netzaufbau für Rettungseinsätze

Rettungskräfte bauen bei der Verwendung der *InCo Units* „automatisch“ ein Ad-hoc-Netz auf, wenn sie die Lösch-Schläuche verlegen. Der prozesskonforme Netzaufbau für Feuerwehreinsätze nach dem Interkupplungskonzept ist in Abbildung 3.15 dargestellt.

3.6.1 Inter-Coupling Unit

Der Aufbau einer *InCo Unit* ist in Abbildung 3.16 skizziert. Eine *InCo Unit* besteht aus zwei Kupplungen, welche genau an die Kupplungen der Feuerwehrschläuche angepasst sind, und zwei kurzen Rohrstücken zwischen den beiden Kupplungen. Das innere Rohr hat den gleichen Durchmesser wie ein Feuerwehrschlauch und kann vom Löschwasser durchströmt werden. Das äußere Rohr dient dem Schutz der Router-Hardware. Diese Hardware besteht aus drei Komponenten, einem eingebetteten System (Overo Gumstix), einem WLAN USB Stick mit externer Antenne und einem Akku. Die externe Antenne ist an dem Außenrohr der Dropped Unit montiert und kann dort herausgezogen werden, um die in Kapitel 3.3 untersuchte Mindesthöhe zum Erreichen der maximalen Datenrate zu ermöglichen. Das Funktionsmuster der *InCo Unit* ist in Abbildung 3.17 dargestellt. Als Hardware für den eingebetteten PC wird der ARM-basierte Overo Earth der Firma Gumstix auf dem Summit Erweiterungs-Board verwendet. An diesen wird per USB der D-Link DWA-160 WLAN-Stick angeschlossen. Das System wird von einer USB-Powerbank mit Strom versorgt, welche 2000 mAh mittels einer integrierten LiPo Batterie liefert. Mit einer Stromaufnahme von ca. 380 mA im Bereitschaftszustand und 400 mA während einer WLAN-Übertragung kann das System mit einer Batterieladung für 5 Stunden betrieben werden. Als Betriebssystem wird ein Debian Linux mit einer 3.3.2er Kernel verwendet.

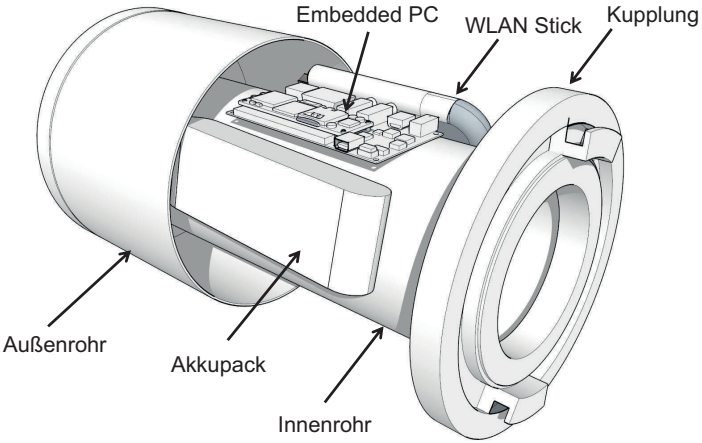


Abbildung 3.16: *InCo Unit* mit teilweise geöffnetem Außenrohr

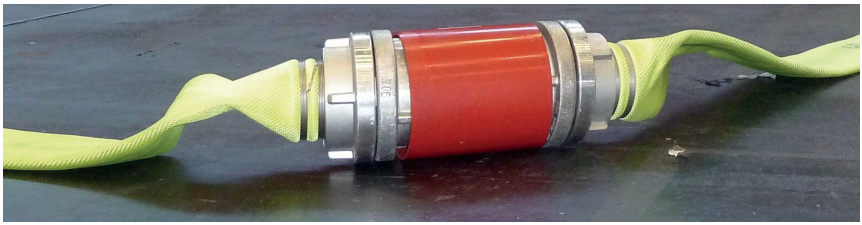


Abbildung 3.17: Funktionsmuster einer *InCo Unit*

3.6.2 Abdeckungsanalyse des Interkupplungskonzepts

Bei der Verwendung der *InCo Units* wird jede 20 m ein WLAN-Router platziert. Wenn nicht durch Hindernisse eine zusätzliche Dämpfung eintritt, können WLAN-Knoten im Freifeld über Entfernungen bis zu 200 m miteinander kommunizieren. Im Rahmen der hier vorgestellten Abdeckungsanalyse soll überprüft werden, ob das häufige Platzieren der *InCo Units* zu der gewünschten WLAN-Abdeckung an einem Einsatzort führt und ob eventuell einige *InCo Units* redundant sind. Um dies zu überprüfen, wird ein exemplarisches Szenario untersucht. Dabei handelt es sich um die Ausstellungshalle Nr. 8 des Messegeländes in Köln. Diese Halle wurde auch im Projekt SPIDER für das Anwendungsszenario ausgewählt.

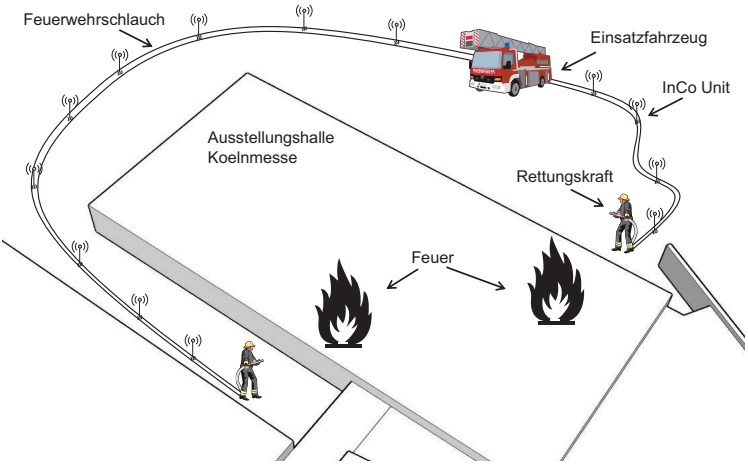


Abbildung 3.18: Modell einer Ausstellungshalle mit Gefahrenstelle

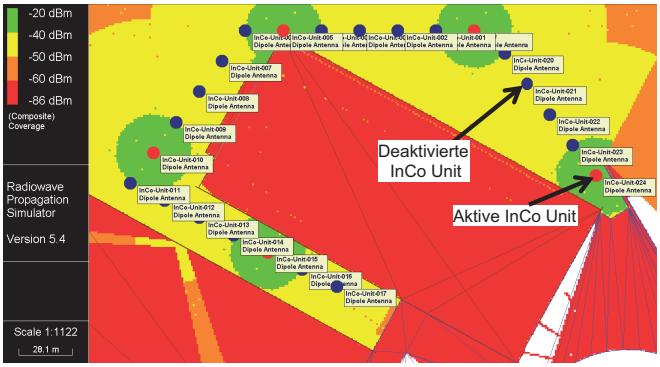
Beschreibung des Anwendungsszenarios

Als Grundlage für die Abdeckungsanalyse wurde zunächst ein 3D-Modell der Messegebäude der Koelnmesse erstellt. Dieses 3D Modell kann dann in den Funkfeldsimulator *RPS* von *Radioplan* importiert werden [16]. In Abbildung 3.18 ist das 3D Modell der Halle 8 dargestellt. In der Darstellung der Halle 8 sind zwei Gefahrenstellen eingezeichnet, die von Rettungskräften beseitigt werden sollen. Es wird angenommen, dass es sich dabei um Feuer handelt, welches gelöscht werden muss. Feuerwehrkräfte rücken mit einem Feuerwehrschlauch zu den Gefahrenstellen aus und nutzen dabei das Interkupplungskonzept und die *InCo Units*, um ein Kommunikationsnetz zwischen Gefahrenstelle und dem Einsatzleiter, der sich in der Nähe des Einsatzfahrzeugs befindet, aufzubauen. Eine Gefahrenstelle befindet sich auf der Rückseite der Halle, weshalb angenommen wird, dass ein besonders langer Schlauch verlegt werden muss. Insgesamt werden 22 *InCo Units* in dem Szenario platziert, um die Rettungskräfte mit dem Einsatzfahrzeug zu verbinden. Bei allen *InCo Units* wird die Kommunikationsantenne soweit herausgezogen, dass die Antennenhöhe keinen Einfluss auf die zu erreichende Datenrate hat.

Ergebnisse der Abdeckungsanalyse

Das Ergebnis der Abdeckungsanalyse ist in Abbildung 3.19(a) dargestellt. Es zeigt, dass die meisten *InCo Units* redundant sind und für eine Abdeckung des Einsatzgebietes nicht benötigt werden. Eine Kommunikation zwischen zwei *InCo Units* ist

(a) Alle *InCo Units* aktiv



(b) Jede 5. *InCo Unit* aktiv

Abbildung 3.19: Abdeckungsanalyse in RPS der Halle 8 der Koelnmesse

bis zu einer Empfangsleistung von −86 dBm möglich. Die Färbung in der Abbildung ist so definiert, dass Empfangsleistungen in vier Farben dargestellt werden. Um die *InCo Units* ist ein Korridor zu erkennen, in dem die Empfangsleistung zwischen −20 dBm und −40 dBm liegt. Dahinter ist eine hellere Fläche zu erkennen, die eine Empfangsleistung von −40 dBm bis −50 dBm darstellt. Durch die häufige Platzierung der *InCo Units* ist eine dunkle Färbung nur in Randbereichen des Szenarios sichtbar. Daran ist zu erkennen, dass viele *InCo Units* redundant platziert wurden.

Um die Überbelegung des Szenarios mit redundanten *InCo Units* zu vermeiden, wird als einfache Regel vorgeschlagen, nur jede fünfte *InCo Unit* zu aktivieren. Diese Strategie soll dazu führen, dass weniger *InCo Units* zu einer vergleichbaren WLAN-Abdeckung am Einsatzort führen.

In Abbildung 3.19(b) ist das Ergebnis der Abdeckungsanalyse zu sehen, wenn nur jede fünfte *InCo Unit* aktiv ist. Anhand der Färbung ist zu sehen, dass sich die aktiven *InCo Units* jeweils noch im Empfangsbereich der benachbarten *InCo Units* befinden. Die vorgeschlagene Regel führt also zum gewünschten Effekt.

Es kann jedoch die Situation eintreten, bei der zwei benachbarte *InCo Units* durch eine Gebäudeecke voneinander getrennt sind, sodass die Multi-Hop-Kommunikation dadurch unterbrochen wird. Somit kann nicht pauschal jede fünfte *InCo Unit* aktiviert werden, während alle anderen *InCo Units* deaktiviert sind. Vielmehr muss dynamisch auf die Umgebung reagiert werden. Ein neuartiger Algorithmus, der in Abhängigkeit der Empfangsleistung der benachbarten *InCo Units* bestimmte redundante *InCo Units* deaktiviert, wird in Kapitel 4 vorgestellt.

3.7 Zusammenfassung

Zuverlässige Kommunikationsnetze mit ausreichender Datenrate für multimediale Anwendungen sind notwendig, damit neue IT-gestützte Dienste für die Unterstützung von Einsatzkräften am Einsatzort realisiert werden können. Öffentliche Datennetze können diese Anforderung im Notfall aufgrund der zunehmenden Anzahl von Panic-Calls oder defekter Infrastruktur nicht erfüllen. Deshalb müssen Feldkräfte ihr eigenes Ad-hoc-Netzwerk aufbauen.

In diesem Kapitel sind zwei Konzepte vorgestellt worden, wie Rettungskräfte beim Aufbau eines Ad-hoc-Netzes unterstützt werden können. In allgemeinen Situationen kann die audiovisuell unterstützte Platzierung eingesetzt werden, bei dem die Rettungskraft mittels einer Ampel und einem akustischen Signal bei der Platzierung von *Dropped Units* unterstützt wird.

Darüber hinaus wurde für spezielle Situationen ein praxisintegrierter Ansatz vorgestellt. Dabei werden die *Dropped Units* in die Schlauchkupplungen von Feuerwehrschläuchen integriert und werden dann als *InCo Units* bezeichnet. Durch die regelmäßige Platzierung der *InCo Units* kommt es *„on-the-fly“* zu einem Netzaufbau. Es kommt dabei aber zu einer Überbelegung mit redundanten *InCo Units*, die möglicherweise die Kommunikation der Rettungskräfte stören. Daher wird im nächsten Kapitel eine Strategie zur Interferenzvermeidung diskutiert.

4

Algorithmen zur Interferenzreduktion in prozesskonform aufgebauten Ad-hoc-Netzen

Im vorangegangenen Kapitel wurde der prozessorientierte Aufbau eines Kommunikationsnetzes mit Hilfe von InCo Units vorgestellt. Wenn Rettungskräfte ein Netz mit InCo Units am Einsatzort aufbauen, so führt dies zu einer Überbesetzung des Szenarios mit redundanten InCo Units, wodurch es zu Interferenzen kommen kann. In diesem Kapitel wird ein Algorithmus vorgestellt, welcher die Interferenzen der redundanten InCo Units reduziert, indem redundante InCo Units deaktiviert werden. Um diesen Algorithmus zu entwickeln, wurden zunächst Algorithmen untersucht, welche die Positionen einzelner Knoten mit Routing Funktionen innerhalb eines Szenarios optimieren. Younis et al. präsentieren in [107] verschiedene Strategien und Techniken für das Platzieren der Knoten in drahtlosen Sensornetzen. In der Literatur wird die optimale Platzierung von Router-Knoten in der Ebene „Steinerbaumproblem mit minimaler Anzahl von Steiner-Punkten und gegebener Kantenlänge“ (engl. Steiner tree problem with minimum number of Steiner points and bounded edge-length - STP-MSPBEL) genannt. Dieses Problem wurde in der Vergangenheit sehr intensiv untersucht. Einen umfassenden Überblick bieten Misra et al. [55]. Nahezu alle Untersuchungen in diesem Problemfeld basieren auf dem Ansatz von Lin und Xue [49], welche ein Schema zur Lösung des Problems liefern, das auf minimalen Spannbäumen basiert. Zur Entwicklung des minimalen Spannbaums können die Algorithmen von Kruskal [45] oder Prim [67] verwendet werden. Die in diesem Kapitel beschriebenen Konzepte und Ergebnisse bauen auf Beiträgen des Autors zur Publikation [102] auf.

4.1 Existierende Knoten-Platzierungs-Algorithmen

Der oben genannte Ansatz zur Lösung des STP-MSPBEL-Problems gilt nur für statische Netze, in denen die Knoten nicht mobil sind. Da sich aber Rettungskräfte normalerweise innerhalb eines Szenarios bewegen, ist ein Lösungsansatz für mobile Netze erforderlich. Die Ergebnisse der hier vorgestellten Untersuchung werden daher mit existierenden Arbeiten von *Huang et al.* verglichen [33], die unterschiedliche Algorithmen für die Platzierung einer minimalen Anzahl von Knoten in mobilen Szenarien vorschlagen. *Huang* stellt zwei heuristische Algorithmen vor,

Tabelle 4.1: Symbole und Abkürzungen

Symbol	Bedeutung
$\mathcal{TS} = \{\mathcal{T}^1 \cdots \mathcal{T}^T\}$	Menge von Netztopologien
$\mathcal{B} = \{B_1 \cdots B_S\}$	Menge der Basisstationen
$\mathcal{L}$	Menge der möglichen Positionen für Knoten
$\mathcal{R}$	Lösung für die Platzierung der Knoten, $\mathcal{R} \subseteq \mathcal{L}$
KPA_m	Knoten-Platzierungs-Algorithmus

den *Topology Stitch Algorithmus* (TSA) und den *Topology Iterative Algorithmus* (TIA), die beide auf Knoten-Platzierungs-Algorithmen basieren, die eine Lösung für statische Netze mit einer Topologie finden können.

Mit Topologie ist in diesem Zusammenhang die räumliche Struktur bzw. Anordnung der verkehrsgenerierenden Quellknoten (Q) innerhalb eines Szenarios gemeint. Diese Knoten Q werden mittels Router-Knoten R an eine Senke S, später auch als Basisstation BS bezeichnet, angeschlossen. Da Q und S zu einem Zeitpunkt t für eine Topologie $\mathcal{T}$ als konstant angenommen werden kann, wird nachfolgend R gemeint, wenn allgemein von Knoten gesprochen wird. Zu unterschiedlichen Zeitpunkten (t_1, t_2, t_3, ...) können sich Q an anderen Orten befinden.

Nachfolgend werden die beiden Algorithmen TSA und TIA detailliert beschrieben. Die Beschreibung basiert auf der Arbeit von *Huang et al.* [33].

4.1.1 Topology Stitch Algorithmus (TSA)

Algorithm 1 Topology Stitch Algorithmus (TSA)

1: **Input:** $\mathcal{TS}, \mathcal{B}, \mathcal{L}$
2: **Output:** Lösung für die Platzierung der Knoten $\mathcal{R}$
3: $\mathcal{R} = \emptyset$
4: **for all** $\mathcal{T}^t$ *in Topology* **do**
5: $\quad \mathcal{R} = \mathcal{R} \cup KPA_m(\mathcal{T}^t, \mathcal{B}, \mathcal{L})$;
6: **end for**
7: Lösche redundante Knoten;

Der *Topology Stitch Algorithmus* (TSA) wird in Algorithmus 1 aufgeführt. Zu Beginn werden die Knoten R für unterschiedliche Zeitpunkte der Topologie unabhängig so platziert, dass eine Verbindung von jedem Knoten Q zu einer BS besteht. Anschließend werden die Positionen der Knoten von allen Zeitpunkten zusammen in eine Ebene kopiert und alle redundanten Knoten gelöscht. Der Reduktionsprozess löscht dabei die Knoten einen nach dem anderen. Nach jeder Löschung wird

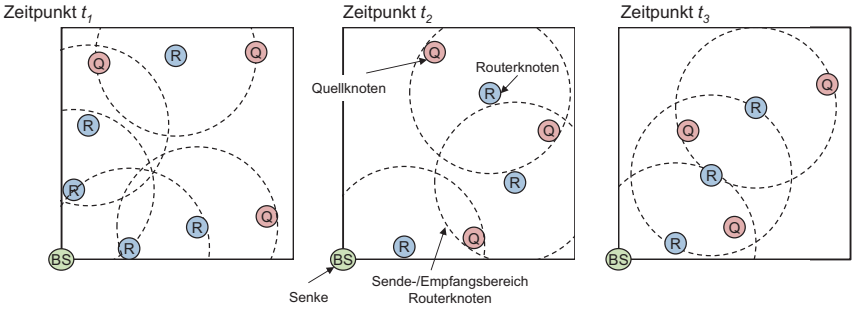


Abbildung 4.1: Topologien eines Szenarios aus drei Quellknoten und einer Senke zu drei Zeitpunkten

überprüft, ob für jeden Knoten Q noch eine Verbindung zu einer BS besteht, und die Löschung wird rückgängig gemacht, falls die Verbindung zur BS verloren gegangen ist. Der TSA nutzt den Reduktionsprozess, um die minimale Anzahl von Knoten zu finden.

Ein Beispiel für die Ausführung des TSA ist in Abbildung 4.1 dargestellt. Es wird die Topologie eines Szenarios für drei unterschiedliche Zeitpunkte gezeigt. Zunächst sind nur die Quellknoten Q und die Senke BS in der Topologie zur jedem Zeitpunkt vorhanden. Q wird mittels möglichst wenigen R mit BS verbunden. Zu jedem Zeitpunkt ergeben sich unterschiedliche Positionen von Q und R.

Die Positionen aller Q und R aller Zeitpunkte werden anschließend in eine einzige Topologie zusammengeführt. Dies ist in Abbildung 4.2 links dargestellt. Diese zusammengeführte Topologie wird nach dem oben beschriebenen Prinzip bereinigt. Die bereinigte Topologie ist in Abbildung 4.2 rechts dargestellt. Es befinden sich keine redundanten R mehr in der Topologie.

4.1.2 Topology Iterative Algorithmus (TIA)

Algorithm 2 Topology Iterative Algorithmus (TIA)

1: $\mathcal{R} = \emptyset$
2: **for all** $\mathcal{T}^t$ *in Topology* **do**
3: $\quad \mathcal{R} = \mathcal{R} \cup KPA^*_m(\mathcal{T}^t, \mathcal{B}, \mathcal{L}, \mathcal{R})$;
4: **end for**
5: Lösche redundante Knoten;

Der *Topology Iterative Algorithmus* (TIA) ist in Algorithmus 2 aufgeführt. Beim TIA wird für jede Topologie ein Knoten nach dem anderen platziert. Dabei wer-

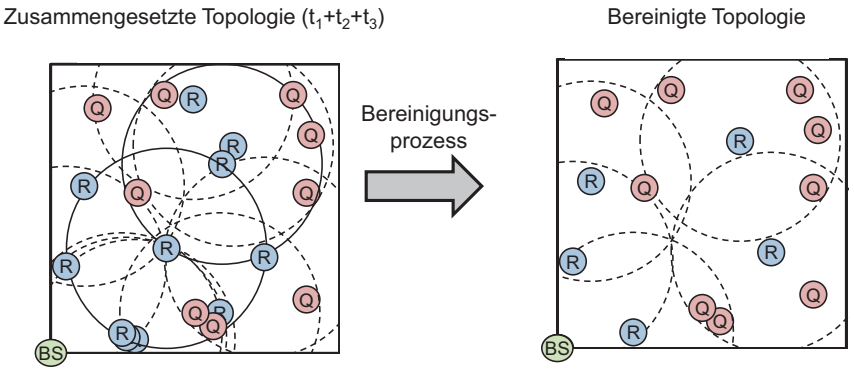


Abbildung 4.2: Zusammengesetze Topologie vor und nach Bereinigungsprozess

den die Positionen der Knoten von vorherigen Topologien mitberücksichtigt. Damit diese Berücksichtigung funktioniert, muss der zusätzliche Parameter $\mathcal{R}$ an den Knoten-Platzierungs-Algorithmus KPA_m übergeben werden. Am Ende der Platzierung der Knoten jeder Topologie werden die redundanten Knoten gelöscht. KPA_m muss so modifiziert werden, dass Knoten aus dem Input-Parameter $\mathcal{R}$ ohne zusätzliche Kosten platziert werden können.

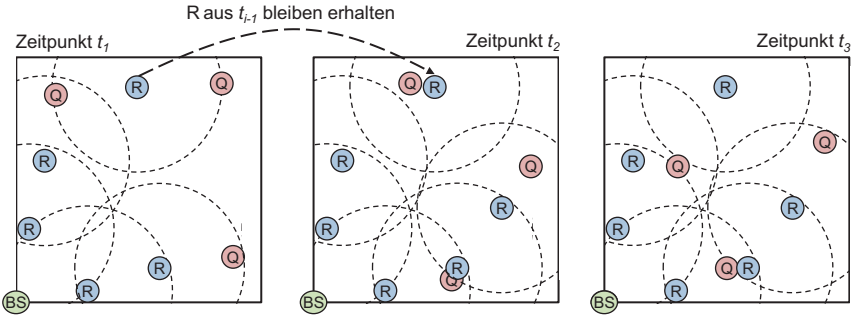


Abbildung 4.3: Beispielhafte Ausführung des TIA

Ein Beispiel für den TIA ist in Abbildung 4.3 dargestellt. Anders als beim TSA sind die einzelnen Zeitpunkte der Topologie nicht unabhängig voneinander. Zum Zeitpunkt t_i platzierte R bleiben für spätere Zeitpunkte $t_j > t_i$ erhalten. So ergibt sich für das Beispiel eine etwas andere Positionierung der R zum Zeitpunkt t_3 im Vergleich zum TSA, bei dem die gleichen Positionen der Q angenommen wurden.

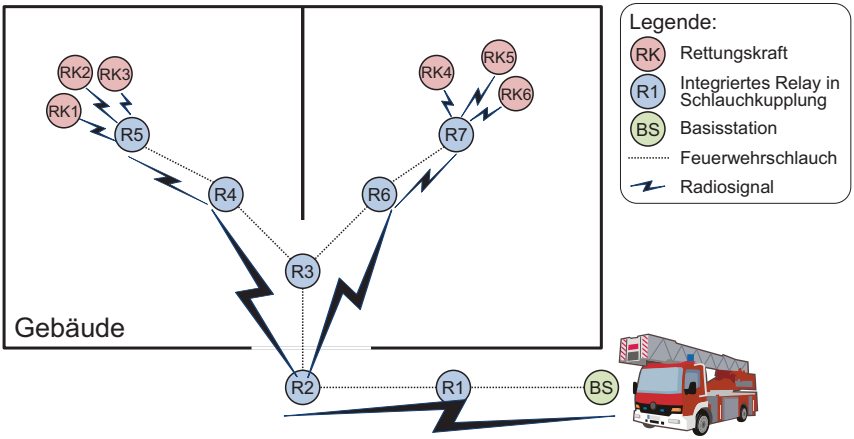


Abbildung 4.4: Netztopologie: Basisstation, InCo Units und Rettungskräfte

Sowohl TSA als auch TIA sind beide Greedy-Algorithmen. Knoten werden platziert, um die Konnektivität bei der gegebenen Topologie zu maximieren. TSA beruht auf dem Reduktionsprozess, bei dem redundante Knoten, die bei der individuellen Optimierung der einzelnen Topologien entstanden sind, bei der Gesamttopologie gelöscht werden. Im Gegensatz zum TSA berücksichtigt der TIA bei der Verarbeitung einer Topologie das Ergebnis einer vorher verarbeiteten Topologie. Dabei wird die Konnektivität durch die in früheren Topologien platzierten Knoten R in $\mathcal{R}$ für die aktuell zu verarbeitende Topologie ausgenutzt. Somit hat die Reihenfolge der Verarbeitung der Topologien durch den TIA einen Einfluss auf die Leistung des Algorithmus.

4.2 Interferenzreduktion bei prozessbedingten Topologien

Werden die in Kapitel 3 vorgestellten *InCo Units* eingesetzt, so führt dies zu einer charakteristischen Netztopologie, die in Abbildung 4.4 schematisch dargestellt ist. Aufgrund der relativ kurzen Länge eines Feuerwehrschlauches (20 m bei einem Schlauch der Größe B in Deutschland) wird eine *InCo Unit* (R) relativ häufig platziert. Bei einem Einsatz stellt ein Löschfahrzeug eine WLAN-Basisstation (BS) zur Verfügung, welche eine Verbindung zu einem Weitverkehrsnetz liefert, z.B. über ein Mobilfunknetz-Gateway oder durch eine Satellitenverbindung. Jede Rettungskraft (RK) pflegt eine Route zur BS, damit sie immer in Kontakt mit dem Einsatzleiter bleibt. Dies führt zu einer Multi-Hop-Verbindung zwischen RK und BS über mehrere *InCo Units*. Häufig werden mehr *InCo Units* platziert als erforderlich, wobei die redundanten *InCo Units* übersprungen werden können. In Abbildung 4.4 können z.B. *InCo Units* R1 und R3 übersprungen werden.

Das Platzieren vieler *InCo Units* kann zu unerwünschten Interferenzen führen. Um diese zu verringern, können redundante *InCo Units* abgeschaltet werden. Dafür können die zuvor genannten TSA und TIA nicht eingesetzt werden, da deren Anwendung bedingt, dass die *InCo Units* an beliebige Orte positioniert werden können. Im Falle des prozessorientierten Ansatzes ergeben sich die Positionen der *InCo Units* jedoch durch den Auslegungsprozess der Feuerwehrschläuche. Es bestehen also weit weniger Freiheitsgrade bei der Positionierung und damit der Auswahl der abzuschaltenden *InCo Units* als bei dem Ansatz von TSA und TIA. Um den Einschränkungen der Positionierung und dem konkreten Charakter der Kommunikationstechnologie gerecht zu werden, wird im Rahmen dieser Arbeit der neuartige „Interferenz-Vermeidungs-Algorithmus“ (IAA) vorgestellt, der die Herangehensweise von TSA und TIA aufgreift und auf die speziellen Anforderungen der hier betrachteten Szenarien abgestimmt ist. Aufgrund der genannten Einschränkungen bei den Freiheitsgraden der Platzierung von *InCo Units* bei der Anwendung des prozessorientierten Ansatzes wird erwartet, dass die Leistungsfähigkeit des IAA in Bezug auf die erforderliche Anzahl von aktiven *InCo Units* ähnliche Ergebnisse, aber nicht bessere, liefert, wie die zuvor eingeführten Algorithmen.

Der IAA nutzt für die Auswahl der zu deaktivierenden, redundanten *InCo Units* die Empfangsfeldstärke (RSS) der benachbarten *InCo Units*. Für die Topologie in Abbildung 4.4 könnten die *InCo Units* R1 und R3 deaktiviert werden. Dies hängt von dem RSS jeder Verbindung im Netz ab. In einem Notfallkommunikationsnetz sind redundante *InCo Units* jedoch wichtig, da die Stromversorgung auf Batterien basiert und daher nur eine begrenzte Laufzeit pro *InCo Unit* besteht. Sobald in der Batterie einer *InCo Unit* keine Energie mehr vorhanden ist und sich die *InCo Unit* abschaltet, reaktiviert der IAA eine zuvor deaktivierte, redundante *InCo Unit*, um die entstandene Lücke im Kommunikationsnetz zu schließen, die durch die leere Batterie entstanden ist.

Algorithm 3 Interferenz-Vermeidungs-Algorithmus (IAA)

Input: $\mathcal{R}$: Menge aller InCo Units im Szenario
Output: $\mathcal{A}$,$\mathcal{I}$: Menge aller aktiven und deaktivierten InCo Units
Initialization: $\mathcal{A} = BS$
repeat
  for all $x \in \mathcal{R}$ sodass $RSS(x, \mathcal{A}) \geq -86\,dBm$ **do**
    if $RSS(x, \mathcal{A}\ )$ ist Kleinster im Empfangsradius **then**
      $\mathcal{A} = \mathcal{A} \cup x$
    else
      $\mathcal{I} = \mathcal{I} \cup x$
    end if
    $\mathcal{R} = \mathcal{R} - x$
  end for
until $R = \emptyset$

Um den Ablauf des IAA mathematisch beschreiben zu können, werden zwei Mengen $\mathcal{A}$ und $\mathcal{I}$ definiert. Dabei repräsentiert $\mathcal{A}$ die aktiven und $\mathcal{I}$ die deaktivierten *InCo Units*. Zu Beginn des IAA sind die beiden Mengen $\mathcal{A}$ und $\mathcal{I}$ leer. Am Anfang wird BS zu $\mathcal{A}$ hinzugefügt und alle redundanten *InCo Units*, die in der Empfangsreichweite von BS sind, werden deaktiviert und zu $\mathcal{I}$ hinzugefügt. Dabei wird genau eine *InCo Unit* nicht deaktiviert. Dieses letzte *InCo Unit* hat die geringste Empfangsfeldstärke und einen RSS größer oder gleich $-86\,\mathrm{dBm}$. Diese *InCo Unit* wird zu der Menge $\mathcal{A}$ hinzugefügt. Der Algorithmus wird so oft wiederholt, bis alle *InCo Units* des Szenarios entweder in $\mathcal{A}$ oder in $\mathcal{I}$ sind.

Der Wert für die Empfangsschwelle ist hardwarespezifisch. Der im Rahmen dieser Arbeit eingesetzte D-Link WLAN-Stick kann im 5 GHz Band bis zu einem RSS von $-86\,\mathrm{dBm}$ Daten empfangen. Das Datenblatt des WLAN-Sticks definiert die in Tabelle 4.2 genannte Datenrate (DR) in Abhängigkeit des RSS. Je schwächer die Signale am Empfänger ankommen, desto weniger Daten können übertragen werden. Die Signale müssen aber mindestens mit einer Feldstärke von $-86\,\mathrm{dBm}$ ankommen, damit eine Kommunikation stattfinden kann.

Tabelle 4.2: Datenrate in Abhängigkeit des RSS am Empfänger für D-Link DWA-160 im 5GHz Modus gemäß Datenblatt [14]

RSS [dBm]	-86	-86	-85	-83	-81	-76	-73	-72
DR [Mbit/s]	6	9	12	18	24	36	48	54

Im Rahmen der hier vorgestellten Untersuchung wird eine zentralisierte Version des IAAs angenommen, welche das gesamte Szenario kennt. Wird der IAA in Kombination mit einem Routing-Algorithmus, beispielsweise OLSR, eingesetzt, kann auch Mobilität im Netz unterstützt werden. Je nachdem, wo sich die aktiven Knoten im Netz befinden, können unterschiedliche *InCo Units* aktiviert werden. Fällt eine *InCo Unit* aus, z.B. wegen einer unzureichenden Stromversorgung, so wird eine deaktivierte *InCo Unit* reaktiviert, welches die ausgefallene *InCo Unit* ersetzt. Diese Funktionalität kann durch passives Scannen und der Analyse des Verkehrs im Netz durch die inaktiven *InCo Units* realisiert werden. Somit ist eine deaktivierte *InCo Unit* in $\mathcal{I}$ zwar nicht in die Multi-Hop-Kommunikation eingebunden, aber es analysiert z.B. alle 30 Sekunden den Verkehr des Netzes und kann auf etwaige Engpässe mittels Reaktivierung reagieren.

Eine konkrete Realisierung könnte auf der Beobachtung der periodisch versendeten *Hello*-Nachrichten der benachbarten *InCo Units* basieren. Im Rahmen dieser Arbeit werden vornehmlich proaktive Routing-Protokolle für die Vernetzung der *InCo Units* eingesetzt. Dabei kommen insbesondere OLSR und BATMAN zum Einsatz. Beide Protokolle versenden regelmäßig Nachrichten, deren Häufigkeit von einer deaktivierten *InCo Unit* beobachtet werden könnte. Wenn die regelmäßigen

Nachrichten ausbleiben, kann sich die deaktivierte *InCo Unit* reaktivieren, um die entstandene Kommunikationslücke zu füllen.

4.3 Leistungsbewertung

4.3.1 Szenarienbeschreibung und Methode

Für die Leistungsbewertung werden vier unterschiedlich große Szenarien betrachtet, in denen eine unterschiedliche Anzahl von Rettungskräften verteilt werden (siehe Tabelle 4.3). In jedem Szenario werden zwei Basisstationen (BS) in der unteren linken (BS1) und der oberen rechten Ecke (BS2) platziert. Im Rahmen dieser Untersuchung wird angenommen, dass sich Rettungskräfte (RK) auf direktem Weg vom Löschfahrzeug (BS) zu ihrer zugewiesenen Position bewegen. Ferner wird angenommen, dass jede RK einen eigenen Schlauch vom Löschfahrzeug mitführt. Somit befinden sich die *InCo Units* entlang einer Geraden zwischen BS1 oder BS2 und RK. Ein beispielhaftes Szenario ist in Abbildung 4.5 dargestellt.

Für jedes Szenario werden zwei unterschiedliche Umgebungen untersucht. Bei der einen Umgebung treten wenige Reflexionen der Funkwellen auf, was für ländliche Gebiete angenommen werden kann. Bei der zweiten Umgebung treten mehr Reflexionen auf, wie es in bebauten Gebieten vorkommen kann. Um die beiden Umgebungen zu differenzieren, wird jeweils ein bestimmter Ausbreitungskoeffizient γ angenommen, der für die Berechnung der Empfangsleistung verwendet wird. *Walke* schreibt in [92], dass realistische Werte für γ „zwischen 2 (Freiraumausbreitung) und 5 (starke Dämpfung z.B. bei städtischer Bebauung)“ liegen. Für die Umgebung mit mehr Reflexionen wird ein γ von 3,29 angenommen, für die Umgebung mit weniger Reflexionen wird $\gamma = 2,87$ gewählt. Für die weitere Untersuchung wird angenommen, dass keine weiteren Störungen auftreten. Unter Berücksichtigung der Sendeleistung P_S, der minimalen Empfangsleistung P_E und der Frequenz f kann daraus die maximale Reichweite r zwischen zwei Kommunikationsknoten berechnet werden. Dazu wird die Formel aus Gleichung 4.1 verwendet.

$$
\begin{aligned}
P_E[dBm] &= P_S[dBm] - F[dB] + G_S[dB] + G_E[dB] \\
F &= \left(\frac{4\pi \cdot f}{c}\right)^2 \cdot r^{\gamma} \\
F[dB] &= 10 log_{10} F \\
r &= \sqrt[\gamma]{10^{\frac{P_S[dBm] - P_E[dBm] + G_S[dB] + G_E[dB]}{10}} \cdot \left(\frac{c}{4\pi \cdot f}\right)^2}
\end{aligned}
\tag{4.1}
$$

Der im Rahmen dieser Arbeit eingesetzte WLAN-Stick DWA-160 sendet laut Datenblatt mit einer Leistung von 16 dBm und hat einen Antennengewinn von 2 dB [14]. Die minimale Empfangsleistung P_E beträgt -86 dBm. Bei einer Frequenz f von 2,4 GHz und einer Ausbreitungsgeschwindigkeit c von $3 \cdot 10^8 \frac{m}{s}$ kann die maximale Entfernung für die beiden Umgebungen wie folgt berechnet werden.

$$\begin{aligned} r_1 &= \sqrt[3,29]{10^{10,6} \cdot \left(\frac{0,3}{9,6\pi}\right)^2}\ m \\ &= 101,1m \approx 100m \end{aligned} \tag{4.2}$$

$$\begin{aligned} r_2 &= \sqrt[2,87]{10^{10,6} \cdot \left(\frac{0,3}{9,6\pi}\right)^2}\ m \\ &= 198,6m \approx 200m \end{aligned} \tag{4.3}$$

Für jedes Szenario werden die beiden Reichweiten 100 m und 200 m untersucht.

Die Positionen der Clients (RK) sind in den Szenarien jeweils gleichverteilt. Zwar sind in einem realen Einsatz die Positionen der Rettungskräfte nicht gleichverteilt, sondern eher auf wenige Positionen, z.B. in der Nähe von Brandherden, konzentriert, jedoch führt dies zu einer Clusterbildung, was einen Einfluss auf den Effekt der unterschiedlich großen Szenarien und die unterschiedliche Anzahl der Rettungskräfte in den Szenarien hat. Die Clusterbildung führt dazu, dass weniger *InCo Units* benötigt werden, da nur noch eine Multi-Hop-Verbindung von einer BS zum Cluster benötigt wird. In der realen Löschsituation werden demnach weniger Verbindungen als im hier verwendeten Modell benötigt. Durch die angenommene Gleichverteilung können jedoch die im Rahmen dieser Arbeit entstandenen Ergebnisse mit Ergebnissen aus der Arbeit von *Huang et al.* [33] verglichen werden.

Jedes Szenario wird 500 Mal untersucht, wobei jeweils neue Positionen der Rettungskräfte gleichverteilt gewählt werden. Die benötigte Anzahl der *InCo Units* für jedes Szenario ist der Mittelwert der berechneten Ergebnisse. Die Parameter der vier Szenarien sind in Tabelle 4.3 dargestellt. Diese Parameter erlauben einen direkten Vergleich mit den Ergebnissen, die von *Huang et al.* [33] vorgestellt wurden. In einem realen Szenario können, je nach Schadenslage, viel mehr Rettungskräfte im Einsatz sein. Die hier gemachten Annahmen erlauben jedoch eine Vergleichbarkeit der Ergebnisse.

Im Rahmen dieser Untersuchung werden einfache Szenarien ohne Hindernisse untersucht. Dies erlaubt einen einfachen Vergleich des hier vorgestellten *InCo Unit* Konzepts mit existierenden Knoten-Platzierungs-Algorithmen.

Tabelle 4.3: Parameter der Szenarien

Szenario	Grundfläche	Quellknoten
1	400m · 400m	4
2	600m · 600m	9
3	800m · 800m	16
4	1000m · 1000m	25

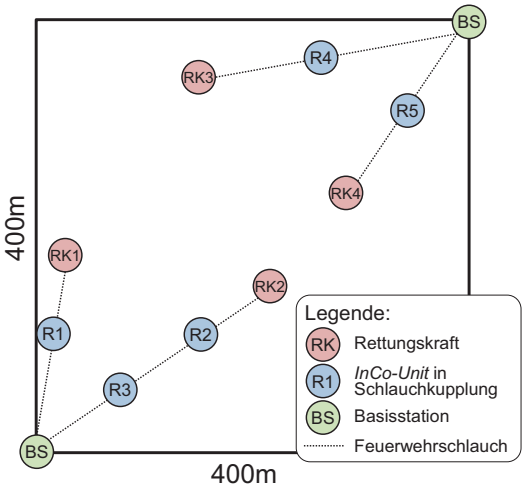


Abbildung 4.5: Beispielhafte Platzierung von InCo Units im Szenario 1

4.3.2 Anzahl benötigter Knoten

Abbildung 4.5 zeigt eine beispielhafte Lösung für die Platzierung der *InCo Units* für das Szenario 1. Weil jede Rettungskraft, bzw. jeder Trupp, ihren eigenen Feuerwehrschlauch auslegt, sind möglicherweise redundante *InCo Units* vorhanden. Diese redundanten *InCo Units* werden durch den IAA deaktiviert. Da die *InCo Units* nicht beliebig positioniert werden, sondern sich ihre Position durch die Verlegung des Feuerwehrschlauches ergibt, liefert der *InCo Units*-Ansatz in Kombination mit dem IAA eine eher überhöhte Anzahl der benötigten *InCo Units*. Daher wird erwartet, dass unter Verwendung des IAAs mehr *InCo Units* platziert werden, als bei den Algorithmen, welche die Anzahl der benötigten Knoten (R, siehe oben) optimieren.

Der IAA wird von einer zentralen Instanz ausgeführt, welche die Netztopologie kennt. Verwaltet werden die einzelnen *InCo Units* in einer Matrix, welche die Anzahl der im Szenario befindlichen *InCo Units* als Spalten aufweist und in den Zeilen

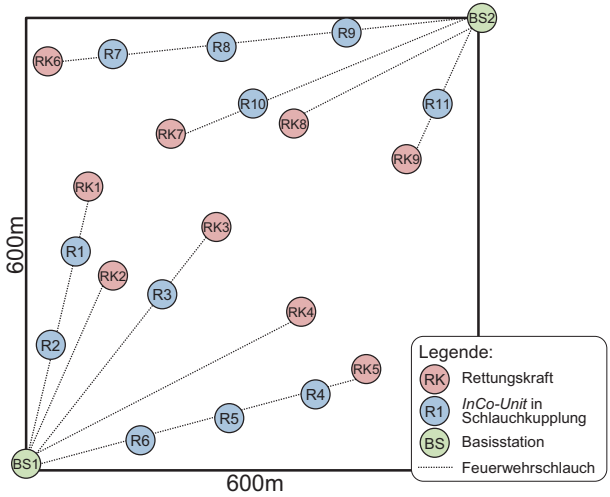


Abbildung 4.6: Beispielhafte Platzierung von InCo Units im Szenario 2

die einzelnen *InCo Units* nach Anzahl der Hops zur Basisstation sortiert. Nachdem die Feuerwehrschläuche ausgebracht wurden, bzw. die Netztopologie feststeht, entfernt der IAA die redundanten *InCo Units*, indem in der Matrix zeilenweise nach benachbarten *InCo Units* gesucht wird. Es wird dann der Nachbar als nächster Hop gewählt, der Teil des längsten Schlauchs dieser Nachbarn ist. Dies führt dazu, dass die *InCo Units* in längeren Schläuchen aktiv bleiben, während der Verkehr, der von Rettungskräften an kurzen Schläuchen erzeugt wird, über die *InCo Units* von längeren Schläuchen geroutet ist. Beispielhaft sei dazu die Abbildung 4.6 angeführt. In dieser Abbildung ist zu sehen, dass am Schlauch von RK2 keine *InCo Unit* aktiv ist. Der Verkehr von RK2 wird über R1 und R2 zur BS1 geroutet. Ebenso ist dies bei RK4 der Fall. RK4 routet den Verkehr über R4, R5 und R6 an BS1.

4.3.3 Vergleich zu existierenden Platzierungsverfahren

Um die Leistung des in diesem Kapitel vorgestellten *Interference Avoidance Algorithm* bewerten zu können, werden die aktiven *InCo Units* der verschiedenen Positionierungsalgorithmen miteinander verglichen, die benötigt werden, um die Rettungskräfte im Szenario mit einer der beiden Basisstationen zu verbinden.

Ziel der Leistungsbewertung ist es zu zeigen, dass die prozesskonforme Vernetzung in Kombination mit dem IAA eine ähnliche Anzahl von aktiven *InCo Units* für die Anbindung der Rettungskräfte erfordert wie optimierende Verfahren. Darüber hinaus soll gezeigt werden, dass die Verwendung des IAA deutliche Vorteile in Bezug

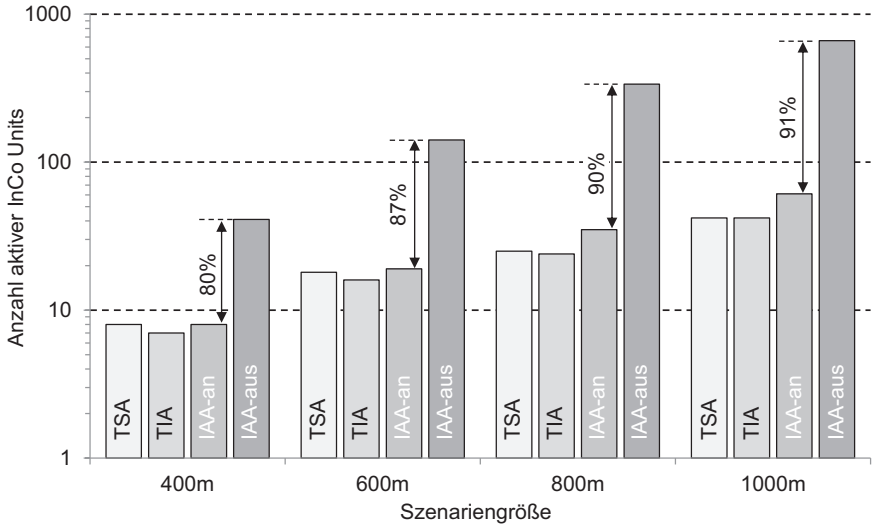


Abbildung 4.7: Anzahl aktiver InCo Units zur Vernetzung mit einer Basisstation bei 100m Reichweite

auf die Anzahl der aktiven *InCo Units* gegenüber dem reinen prozessintegrierten Ansatz ohne IAA bringt.

In Abbildung 4.7 ist die benötigte Anzahl von aktiven *InCo Units* in Abhängigkeit der Szenariengröße bei einer Übertragungsreichweite von 100 m dargestellt. Die optimierenden Verfahren TSA und TIA benötigen im 400 m großen Szenario ungefähr sieben Router-Knoten für die Vernetzung. Das hier vorgestellte prozesskonforme Vernetzungskonzept mit aktivem IAA (IAA_{an}) benötigt mit acht aktiven *InCo Units* eine vergleichbare Anzahl. Wird der IAA nicht verwendet, so steigt die Anzahl der aktiven *InCo Units* auf das fünffache an, da in diesem Fall jede *InCo Unit* aktiv ist. Der IAA bringt in diesem Szenario eine Ersparnis an aktiven *InCo Units* von 80 %.

Im zweiten Szenario mit einer Kantenlänge von 600 m benötigen die optimierenden Verfahren im Durchschnitt 17 Router-Knoten. Die prozesskonforme Vernetzung mit aktivem IAA benötigt hierzu 19 *InCo Units*. Ohne aktiven IAA sind 141 *InCo Units* aktiv. Somit bringt der IAA eine Ersparnis von ca. 87%. Demnach benötigt der IAA eine sehr ähnliche Anzahl von *InCo Units* wie die optimierenden Verfahren in diesem Szenario und ist dabei praxistauglich.

Für die beiden großen Szenarien mit 800 m und 1000 m Größe sieht das Ergebnis ähnlich aus. Der Unterschied liegt lediglich darin, dass der aktive IAA nicht mehr ganz mit den optimierenden Algorithmen mithalten kann. So werden im 800 m

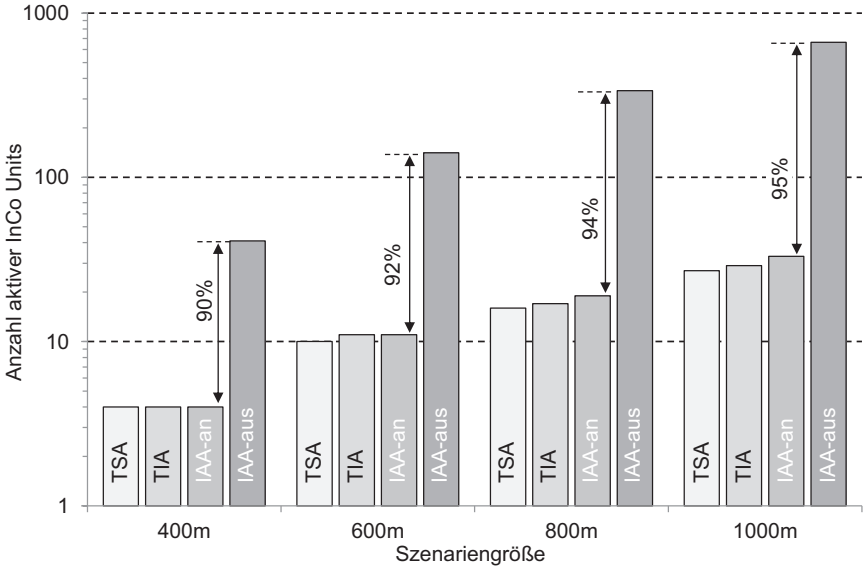


Abbildung 4.8: Anzahl aktiver InCo Units zur Vernetzung mit einer Basisstation bei 200m Reichweite

Szenario ca. 10 *InCo Units* mehr benötigt als bei TSA und TIA. Bei dem größten Szenario sind es sogar ca. 20 *InCo Units* Unterschied zwischen IAA und den optimierenden Verfahren. Dieser Unterschied liegt in der Optimierung begründet, die TSA und TIA auszeichnet. Der IAA kann die Positionen der *InCo Units* nicht frei wählen, sondern nur die Positionen der Schlauchkupplungen verwenden. Die Aktivierung des IAA gegenüber dem *InCo Units*-Konzept ohne IAA bringt in beiden großen Szenarien eine Ersparnis von ca. 90 %.

Wird die Empfangsreichweite auf 200m erhöht, so sinkt die Anzahl der benötigten *InCo Units* für alle Szenarien, wie in Abbildung 4.8 dargestellt. Für das 400 m-Szenario werden bei dieser Reichweite sowohl für die optimierenden Verfahren als auch für die prozesskonforme Vernetzung mit aktivem IAA nur vier aktive *InCo Units* benötigt. Wird der IAA nicht verwendet, so steigt bei der prozesskonformen Vernetzung die Anzahl der aktiven *InCo Units* auf das zehnfache.

Für das 600 m Szenario werden für TSA und TIA 10 bzw. 11 Router-Knoten benötigt. Der IAA erfordert hier ebenfalls 11 *InCo Units*. Wird der IAA nicht verwendet, so steigt die Anzahl der aktiven *InCo Units* in diesem Szenario auf 141. Der IAA bringt somit eine Ersparnis von 92 %.

In den beiden großen Szenarien benötigen die optimierenden Verfahren TSA und TIA weniger Router-Knoten als der IAA. Der Unterschied ist jedoch viel kleiner

als zuvor bei einer Empfangsreichweite von 100 m. Im 800 m Szenario beträgt der Unterschied zwischen TSA/TIA und dem IAA zwei und im größten Szenario ca. 5 *InCo Units*. Es wird deutlich, dass der Vorteil der optimierenden Verfahren bei steigender Empfangsreichweite sinkt. Die Ersparnis des IAA im Vergleich zum *InCo Units*-Verfahren ohne IAA beträgt bei beiden großen Szenarien ca. 94 %.

Die Ergebnisse führen zu dem Schluss, dass der im Rahmen dieser Arbeit vorgestellte *InCo Unit*-Ansatz mit aktivem IAA im Vergleich zu optimierenden Verfahren für die hier untersuchten Szenarien eine ähnliche Anzahl von aktiven Knoten für die Vernetzung der Rettungskräfte mit einer Basisstation benötigt. Großer Vorteil des *InCo Unit*-Ansatzes mit aktivem IAA ist die Praxistauglichkeit. Auch wenn die optimierenden Verfahren in manchen Situationen weniger aktive Knoten benötigen, so ist aufgrund der Praxistauglichkeit die Verwendung des *InCo Units*-Ansatz mit aktivem IAA bei vergleichbaren Szenarien empfehlenswert. Der prozesskonforme Ansatz ohne IAA führt zu einer viel größeren Anzahl von aktiven *InCo Units* im Netz, was zu Interferenzen führen kann.

Unter Berücksichtigung der gewünschten Ausfallsicherheit und der in den *InCo Units* eingesetzten Batterien ist festzuhalten, dass die Redundanz, die durch die Verwendung der *InCo Units* in das Netz hineingebracht wird, sich positiv auswirken kann. Ausfälle einzelner *InCo Units* können durch Reaktivierung benachbarter *InCo Units*, falls diese vorhanden sind und über eine ausreichende Energieversorgung verfügen, kompensiert werden. Darüber hinaus ist anzunehmen, dass bei steigendem Bedarf der Preis pro *InCo Unit* sinken wird, was für den Einsatz bei der Feuerwehr ein wichtiges Entscheidungskriterium ist.

4.4 Zusammenfassung

In diesem Kapitel wird ein neuartiger Algorithmus zur Interferenzreduktion bei der Verwendung von *InCo Units* vorgestellt, welcher zum Ziel hat, Rettungskräfte beim Aufbau eines Ad-hoc-Netzes zu unterstützen, ohne sie dadurch bei der Wahrnehmung ihrer angestammten Aufgaben zu behindern. Wird der hier vorgestellte Interferenz-Vermeidungs-Algorithmus eingesetzt, so ist die Anzahl der benötigten aktiven *InCo Units* in den untersuchten Szenarien nur geringfügig höher als bei der Positionierung der Knoten an zuvor mittels optimierenden Algorithmen berechneten Orten. Wird berücksichtigt, dass Feuerwehrleute im Normalfall nicht wissen, wo sich die optimalen Orte für die Knoten befinden, und dass sie keine Zeit haben die Knoten an dafür speziell berechneten Orten abzulegen, so stellt das hier vorgestellte *InCo Units*-Konzept in Verbindung mit dem IAA eine geeignete Lösung zur Vernetzung der Rettungskräfte dar, welches sich praxisnah in ihren Arbeitsprozess integrieren lässt.

5

Dienstgüte für den Katastrophenschutz

Im vorherigen Kapitel wurde gezeigt, wie ein Kommunikationsnetz für Rettungskräfte prozesskonform aufgebaut werden kann. Aufgrund der weiten Verbreitung von WLAN kann davon ausgegangen werden, dass andere WLAN-Netze schon am Einsatzort vorhanden sind. Es wird angenommen, dass diese am Einsatzort vorhandenen WLAN-Netze das neu aufgebaute Ad-hoc-Netz der Rettungskräfte stören können. Ferner wird angenommen, dass die Rettungskräfte nicht auf das am Einsatzort vorhandene WLAN-Netz zugreifen können. Darüber hinaus werden von den Rettungskräften unterschiedliche Dienste verwendet, die verschiedene Anforderungen an das Kommunikationsnetz haben. Im Rahmen dieses Kapitels wird ein Konzept vorgestellt, welches eine Priorisierung der Kommunikation der Rettungskräfte gegenüber existierenden Netzen am Einsatzort ermöglicht. Darüber hinaus erlaubt das Konzept die gezielte Priorisierung einzelner Dienste, um damit Dienstgüte bereitzustellen.
Die in den Abschnitten 5.4 und 5.5 dieses Kapitels beschriebenen Konzepte und Ergebnisse bauen auf Beiträgen des Autors zur Publikation [101] auf.

5.1 Einleitung

Wenn der Erfolg einer Rettungsaktion vom effizienten Einsatz eines Entscheidungs-Unterstützungssystems abhängt, so ist die Zuverlässigkeit des Kommunikationsnetzes zwingend erforderlich. Daher muss das Kommunikationsnetz gewisse Dienstgütekriterien erfüllen.

Der Aufbau und Einsatz eines Ad-hoc-WLAN-Netzes kann aufgrund von schon vorhandenen WLAN-Netzen gestört werden. Diese Störungen sind nicht vernachlässigbar, da in Deutschland im 2,4 GHz-Band nur drei überlappungsfreie Kanäle zur Verfügung stehen. Exemplarisch ist in Abbildung 5.1 die Kanalbelegung an der TU Dortmund im 2,4 GHz Band dargestellt. Die Kanalbelegung wurde mit dem *Wi-Spy 2.4x* Kanalanalysator der Firma *metageek* gemessen [52].

Am Einsatzort wetteifern bestehende WLAN-Netze mit dem neu aufzubauenden Ad-hoc-Netz um den Zugang zum Funkkanal. Um den Rettungskräften einen Vorteil zu verschaffen, wird im Rahmen dieser Arbeit eine Anpassung der IEEE 802.11

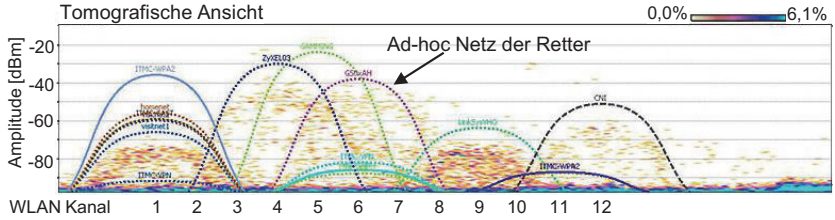


Abbildung 5.1: Kanalbelegung an der TU Dortmund im 2,4 GHz Band

DCF-Parameter vorgeschlagen. Da die Ergebnisse der Arbeit auch experimentell umgesetzt werden sollen, wurde auf 802.11b/g aufgesetzt, da hierfür offene Implementierungen vorhanden sind.

Die Anpassung der MAC-Parameter erlaubt nicht nur die Priorisierung der Rettungskräfte, sondern auch die Einteilung der Sendedaten in unterschiedliche Kategorien. Diese Einteilung erlaubt eine kategoriespezifische Behandlung von Diensten. Daher kann je nach Dienst eine bestimmte Dienstgüte unterstützt werden, die auf spezifisch modifizierten MAC-Parametern beruht. Die *IEEE 802.11e*-Erweiterung [37] fügt Dienstgüte für Heimanwendungen, wie beispielsweise VoIP oder Videostreaming, zu WLAN hinzu. Während die bei IEEE 802.11e eingeführten Zugriffskategorien Multimedia-Anwendungen gut unterstützen, sind für Szenarien im Katastrophenschutz eigene, spezifische Zugriffskategorien notwendig. Im Rahmen dieser Arbeit werden fünf neuartige Zugriffskategorien auf Basis der DCF aus 802.11b/g eingeführt, welche die Anforderungen der Rettungskräfte, insbesondere von Feuerwehrleuten, adressieren. Die Anforderungsanalyse wurde in Zusammenarbeit mit Mitarbeiten der Feuerwehr Gelsenkirchen im Rahmen des vom BMBF geförderten Projekts SPIDER [85] durchgeführt.

5.2 Mögliche Priorisierung für Rettungskräfte

Verschiedene Verfahren ermöglichen den störungsarmen Betrieb eines Kommunikationsnetzes für Rettungskräfte. Dazu zählt unter anderem ein Frequenzwechsel der WLAN-Kommunikation hin zu einem dedizierten Spektrum, welches nur von Rettungskräften verwendet werden darf. Ferner könnte durch eine zentrale Instanz, basierend auf IEEE 802.11e, jeder Rettungskraft ein bestimmter AIFSN-Wert zugewiesen werden, wobei CW_{min} und CW_{max} auf 1 festgelegt werden [72]. Darüber hinaus können auf Basis von IEEE 802.11e neue Kategorien mit dazugehörigen Parametern eingeführt werden.

Kuo et al. schlagen in [46] eine einfache Möglichkeit vor, Dienstgüte mittels einer verzögerten Wettbewerbsphase zu realisieren. Die Leistungsbewertung ihres DC-

DCF genannten Verfahrens basiert ebenso wie das analytische Modell der hier vorgestellten EDCF auf der Markov-Kette von *Bianchi* [5].

5.2.1 Betrieb im dedizierten Spektrum

Die WLAN-Kommunikation von Rettungskräften in ein dediziertes Spektrum zu verlagern ist zwar prinzipiell technisch möglich, jedoch aufgrund des belegten Funk-Spektrums kaum realisierbar. Funkspektrum ist extrem kostbar, das durch die Auktionen der Mobilfunklizenzen demonstriert wurde [21]. Die Behörden und Organisationen mit Sicherheitsaufgaben (BOS) besitzen zwar schon eigene Frequenzen, welche jedoch für den Sprechfunk eingesetzt werden.

Darüber hinaus sind für einen Frequenzwechsel Anpassungen an der Hardware notwendig. Soll beispielsweise in einem niedrigeren Frequenzband gefunkt werden, so wird eine an die Frequenz angepasste Antenne notwendig. Somit sind spezielle Hardware-Lösungen notwendig, welche die Nutzung von Standardkomponenten ausschließen. Dieses führt zu höheren Kosten.

Da sowohl zusätzliche Funkfrequenzen, als auch angepasste Hardware zusätzliche Kosten verursachen, wird von dieser Möglichkeit abgesehen, obwohl die dedizierte Nutzung die beste Priorisierung erbringen würde.

5.2.2 Priorisierung durch dedizierte AIFSN

Für Multimedia-Kommunikation schlagen *Schilling et al.* vor [72], den Zufallszugriff auf den WLAN-Kanal zu deaktivieren und stattdessen einen deterministischen Zugriff zu verwenden. Der Zufallszugriff sorgt dafür, dass die WLAN-Nutzer im Mittel gleichhäufig auf den Kanal zugreifen können. Sollen die Nutzer nun jedoch priorisiert auf den Kanal zugreifen, so wird ihnen bei diesem Verfahren gemäß ihrer Priorität ein dedizierter AIFSN-Wert zugewiesen. Kommt es zu konkurrierenden Übertragungswünschen, so wird der Nutzer auf den Kanal zugreifen können, der den niedrigeren AIFSN-Wert hat. Gleiche Werte für den AIFSN sind dabei nicht möglich, um Kollisionen auszuschließen. Diese Art der Priorisierung wird hier nicht verwendet, da angenommen wird, dass eine dedizierte Zuweisung der AIFSN-Werte für jede Rettungskraft bei einem Einsatz nicht praktikabel ist.

5.2.3 Neue Zugriffskategorien auf Basis von IEEE 802.11e

Die günstigste Alternative, die ohne Modifikation der Hardware und ohne eine dedizierte Parametrisierung für jede Rettungskraft auskommt, ist die Einführung von neuen Zugriffskategorien auf Basis von IEEE 802.11e. Dieses Verfahren wurde in [101] veröffentlicht und soll anschließend detailliert erläutert werden.

5.3 Neuartige Priorisierungskategorien

Das Ziel des hier vorgestellten Priorisierungs- und Dienstgüteschemas ist die Steigerung der Datenrate der Einsatzkräfte in Wettbewerbssituationen mit herkömmlichen WLAN-Nutzern, bei minimaler Anpassung der existierenden Technologien. Diese Rahmenbedingungen sind aus der Anforderungsanalyse abgeleitet, welche in Kooperation mit der Feuerwehr Gelsenkirchen im Projekt SPIDER durchgeführt wurde. Die Anforderungsanalyse führt zu den in Tabelle 5.1 vorgeschlagenen Priorisierungskategorien (engl. *Access Category* AC).

Tabelle 5.1: Vorgeschlagene Priorisierungskategorien

Prio.	Name	Beschreibung
AC1	Dynamisches Video	Video Ströme von bewegten Kameras
AC2	Statisches Video	Video Ströme von stationären Kameras
AC3	Sprache	Sprachkommunikation
AC4	Sensordaten	Sensor- und Positionsdaten
AC5	Hintergrund	Datei und sonstiger Datentransfer

5.4 Optimierung der EDCF Parameter

Um die Priorisierungskategorien aus Tabelle 5.1 zu unterscheiden und unterschiedlich zu gewichten, wurden die Parameter, die vornehmlich für den Zufallszugriff auf den Kommunikationskanal verantwortlich sind, angepasst. Konkret wurden die beiden Parameter des Wettbewerbsfensters (engl. *Contention Window* - CW) $\mathrm{CW}_{\mathrm{min}}$ und $\mathrm{CW}_{\mathrm{max}}$ verringert und darüber hinaus der *Short Interframe Space* $SIFS$ der IEEE 802.11 DCF verkürzt. Die angepasste Funktion wird Emergency-DCF (EDCF) genannt. Nutzer im Kommunikationsnetz, welche die EDCF einsetzen, können mit einer deutlich höheren Wahrscheinlichkeit während der Wettbewerbsphase auf den Kanal zugreifen.

Nachfolgend wird zunächst die Modifikation der SIFS-Werte und anschließend die Anpassung der Wettbewerbsfenster für die einzelnen Zugriffskategorien beschrieben.

5.4.1 Anpassung der SIFS Werte

Für die Differenz zweier SIFS Werte Δ_{SIFS} unterschiedlicher Zugriffskategorien (ACs) wurde ein minimaler Abstand von $1\mu s$ gewählt. Aufgrund der Freiraumaus-

breitung ergibt sich somit zwischen Stationen folgender maximaler Abstand d_{max}, der die Priorisierung durch unterschiedliche SIFS-Werte erlaubt:

$$c \approx 300.000.000 \frac{m}{s} = 300 \frac{m}{\mu s} \tag{5.1}$$

$$d_{max} = \Delta_{SIFS} \cdot c \tag{5.2}$$

$$= 1\mu s \cdot 300 \frac{m}{\mu s} = 300m \tag{5.3}$$

Ein Abstand von 300 m stellt eine akzeptable obere Schranke dar, die einen Einsatz der Priorisierung der EDCF in der Praxis kaum einschränkt. Die gewählten SIFS Werte weichen nicht gravierend vom Standard ab. Bei IEEE 802.11 b/g ist ein SIFS laut Standard $10\mu s$ lang [40].

Im Rahmen der später folgenden Leistungsbewertung wurde ein Simulationsmodell von IEEE 802.11b/g verwendet. Daher werden hier die Parameter für den Standard IEEE 802.11b/g als Ausgangswerte angenommen [40]. Konkret bedeutet dieses für den SIFS einen Ausgangswert von $10\mu s$ als obere Grenze für die angestrebte Priorisierung.

Bei der Überlegung, den SIFS zu verkürzen, um eine Priorisierung zu ermöglichen, darf der SIFS Wert nicht beliebig abgesenkt werden. Es müssen Verzögerungen bei der Verarbeitung der Daten einkalkuliert werden. Im Standard wird *aSIFSTime* als Summe der drei Verarbeitungsverzögerungen von RF, PLCP und MAC, plus der *turnaround time* definiert [40]. Die Verarbeitung in der MAC-Schicht und die *turnaround time* sollen jeweils weniger als $2\mu s$ dauern. Die Verzögerungen durch die Verarbeitung im RF-Teil und der PLCP sind abhängig von der Implementierung des Herstellers, sollen aber weit weniger als $4\mu s$ benötigen. In der Summe ergibt sich daraus eine Untergrenze für *aSIFStime* von $8\mu s$.

Daher wurde für $SIFS_{AC1}$ der Wert $8\mu s$ gewählt. Aufgrund des oben genannten Abstands von 300 m ergibt sich für $SIFS_{AC2}$ ein Wert von $9\mu s$. Aufgrund der Obergrenze von $10\mu s$ kann nicht jeder Zugriffskategorie ein eigener SIFS-Wert zugewiesen werden. Daher wird $SIFS_{AC3}$ ebenfalls ein Wert von $9\mu s$ zugewiesen. Die beiden Kategorien AC4 und AC5 teilen sich einen SIFS von $10\mu s$. Die Priorisierung der Zugriffskategorien mit gleichem SIFS wird durch unterschiedliche Größen ihrer Wettbewerbsfenster realisiert.

5.4.2 Anpassung der Wettbewerbsfenster

Die Anpassung der Wettbewerbsfenster der einzelnen Zugriffskategorien ist komplexer als die Anpassung der Short Interframe Space (SIFS), da es hierbei mehr Freiheitsgrade gibt. Das Wettbewerbsfenster ist ein Wertebereich von natürlichen

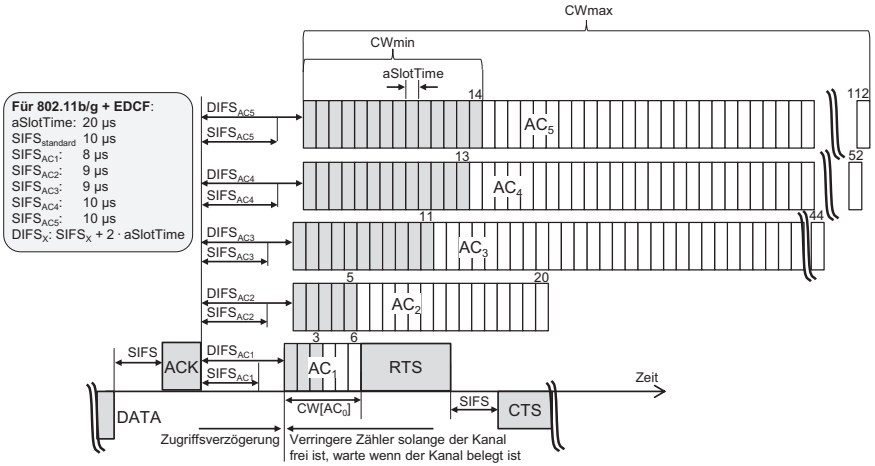


Abbildung 5.2: Timing der EDCF Priorisierungskategorien

Zahlen beginnen bei Null bis zu einer oberen Schranke. Diese obere Schranke startet mit dem Wert $\mathrm{CW}_{\min}$ und wird mit jedem Backoff erhöht, bis die maximale obere Schranke $\mathrm{CW}_{\max}$ erreicht wird. Der Standardwert ist für $\mathrm{CW}_{\max}$ 1023. Für die Zugriffskategorie AC1 sollen kleinere Werte als die von AC_{audio} bei IEEE 802.11e für das Wettbewerbsfenster gewählt werden. Konkret ist bei der AC_{audio} der Parameter $CW_{min} = 7$. Daher wurde bei der $AC1$ der Parameter für $\mathrm{CW}_{\max}$ = 6 gewählt. Der Parameter für $\mathrm{CW}_{\min}$ ergibt sich aus der Hälfte des $\mathrm{CW}_{\max}$ Wertes, also $CW_{min} = 3$ für AC1.

Der $\mathrm{CW}_{\min}$ Wert für AC2 wurde 1 *timeslot* kleiner gewählt als der Wert von $\mathrm{CW}_{\max}$ von AC1, also ist bei der Zugriffskategorie AC2 der Parameter für CW_{min} mit 5 gewählt. Für AC2 bis AC4 wurden zwei exponentielle Backoff-Runden angenommen. Daher ist der Wert $\mathrm{CW}_{\max}$ für AC2 $5 \cdot 2 \cdot 2 = 20$.

Die übrigen Werte für die Größen der Wettbewerbsfenster von AC3 bis AC5 wurden mit Hilfe des Simulators OMNeT++ [32] durch einen iterativen Prozess gefunden, wobei experimentell ermittelt wurde, welche Werte zu der gewünschten Priorisierung und zu einer hohen Datenrate führen. Der Wert für $\mathrm{CW}_{\max}$ ergibt sich dabei aus den Backoff-Runden. Bei AC3 und AC4 wird der $\mathrm{CW}_{\min}$ Wert mit 2^2 multipliziert und bei AC5 mit 2^3, da bei AC5 ein dreistufiger Backoff-Prozess angenommen wurde.

Tabelle 5.2: Parameter der EDCF Zugriffskategorien

Prio.	SIFS [μs]	$\mathrm{CW}_{\mathrm{min}}$ [ts]	$\mathrm{CW}_{\mathrm{max}}$ [ts]
AC1	8	3	6
AC2	9	5	20
AC3	9	11	44
AC4	10	13	52
AC5	10	14	112

Zusammenfassung der EDCF Parameter

Die optimierten Parameter der EDCF sind in Tabelle 5.2 zusammengefasst (ts = *timeslot*). Zusätzlich sind die Parameter der Zugriffskategorien in Abbildung 5.2 grafisch aufbereitet, um die Unterschiede deutlich hervorzuheben. Der Unterschied der Wettbewerbsfenster CW_{min} (grau hinterlegt) und CW_{max} für die einzelnen Zugriffskategorien AC_1-AC_5 fällt dabei viel deutlicher aus als die geringen Unterschiede der SIFS-Werte. Die Wettbewerbsfenster der Zugriffskategorien sind aus mehreren vertikalen Rechtecken zusammengefügt, wobei ein Rechteck einen Timeslot symbolisiert. Ein kleines Wettbewerbsfenster führt im Durchschnitt zu einem raschen Kanalzugriff und damit zu einer hohen Priorität.

5.5 Analytisches Modell der EDCF

Nachfolgend wird das analytische Modell zur Bewertung der EDCF beschrieben, welches vom Modell der EDCA von *Xiong* [103] abgeleitet wurde. In einem ersten Schritt wird der Unterschied zwischen DCF und EDCA beschrieben, um daraus das analytische Modell der EDCF abzuleiten. In einem zweiten Schritt werden die beiden grundlegenden Markov-Ketten vorgestellt, auf denen die folgenden Berechnungen basieren. Anschließend werden die Übergangswahrscheinlichkeiten der Zustände der Markov-Ketten berechnet. Abschließend wird eine geschlossene Lösung für das analytische Modell präsentiert. Grundlagen für das hier präsentierte analytische Modell sind in [4] gelegt worden.

5.5.1 Herleitung des analytischen Modells für die EDCF

Die im Rahmen dieser Arbeit entstandene EDCF hat Gemeinsamkeiten mit der aus IEEE 802.11e bekannten EDCA. Beide Funktionen definieren unterschiedliche Zugriffskategorien mit ihren entsprechenden Prioritäten. Darüber hinaus nutzen beide spezielle *Inter Frame Spacings* (AIFS bei der EDCA und unterschiedliche SIFS, bzw. DIFS bei der EDCF) und unterschiedliche Werte für $\mathrm{CW}_{\mathrm{min}}$ und

CW_{max} . Daher ist es möglich das analytische Modell für die EDCF von der EDCA abzuleiten. Zunächst soll hier noch auf die Unterschiede zwischen der EDCF und der EDCA eingegangen werden: Der erste Unterschied besteht in der Zählweise des Backoffs beim Rückwärtszählen. Im Falle der EDCF wird eine Zahl N zufällig aus dem Wettbewerbsfenster gezogen. Anschließend wird N in jedem Zeitschlitz um eins heruntergezählt. Falls der Kanal als belegt detektiert wird, so wird das Herunterzählen nach der Kanalbelegung mit demselben Wert K fortgesetzt, den der Zähler vor der Kanalbelegung hatte (siehe Abbildung 5.3 oben). Im Falle der EDCA wird das Herunterzählen nach einer Kanalbelegung mit einem um eins reduzierten Zähler $(K-1)$ fortgesetzt (siehe Abbildung 5.3 unten).

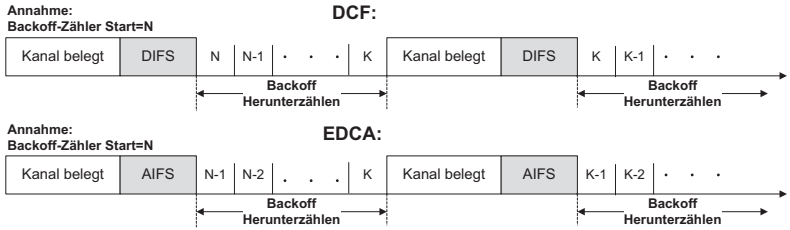


Abbildung 5.3: Regel zum Herunterzählen des Backoffs in DCF und EDCA

Der zweite Unterschied ist der Zeitpunkt, ab wann die Übertragung beginnt, wenn der Backoff Zähler den Zustand Null erreicht. Dieser Unterschied wird in Abbildung 5.4 gezeigt. Im Falle der EDCF startet die Rahmenübertragung im selben Zeitschlitz, wenn der Zähler Null erreicht. Im Falle der EDCA startet die Übertragung einen Zeitschlitz nach dem Erreichen des Zustands Null.

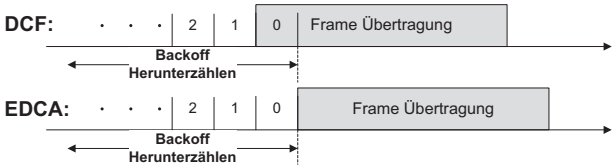


Abbildung 5.4: Zeitpunkt des Starts der Übertragung für DCF und EDCA

Aufgrund dieser Unterschiede wurde das analytische Modell von *Xiong* [103] angepasst, wobei ein etwas verändertes Verhalten nach einer Kanalbelegung und vor einer Übertragung resultiert. Das abgeleitete analytische Modell der EDCF und das entsprechende Gleichungssystem werden im Folgenden hergeleitet und diskutiert.

5.5.2 Zeitdiskrete, zweidimensionale Markov-Modelle

Bei der Modellierung der Markov-Kette, welche die EDCF repräsentiert, muss eine Besonderheit beachtet werden. Diese Besonderheit beruht auf den unterschiedlich langen SIFS-Parametern der einzelnen Zugriffskategorien. Für die Leistungsbewertung der EDCF treten Stationen, die mit unterschiedlichen Zugriffskategorien priorisiert sind, im Wettbewerb gegeneinander an. Wenn die SIFS-Parameter der konkurrierenden Stationen gleich groß sind, dann kann das Verhalten der Stationen mit einer Markov-Kette abgebildet werden. Konkurrieren Stationen miteinander, deren SIFS-Parameter unterschiedlich groß sind, muss dieser Unterschied berücksichtigt werden. Daher wird für die Modellierung der Stationen, die einen höheren SIFS-Parameter im Vergleich zu konkurrierenden Stationen verwenden, eine weitere Markov-Kette benötigt. Mittels dieser zweiten Markov-Kette wird die Priorisierung durch die Unterschiede in den SIFS-Werten berücksichtigt.

Bei der Leistungsbewertung der EDCF werden immer zwei Zugriffskategorien miteinander verglichen. Um nicht alle Kombinationen der Zugriffskategorien einzeln zu beschreiben, werden im Folgenden die Bezeichnungen $\mathrm{AC_A}$ und $\mathrm{AC_B}$ verwendet. Im Wettbewerb von $\mathrm{AC_A}$ mit $\mathrm{AC_B}$ kommt es aufgrund der oben beschriebenen Unterschiede der SIFS bzw. der DIFS ($DIFS = 2 \cdot SIFS + aTimeSlot$) zu zwei möglichen Konstellationen bei der Verteilung der Zeitschlitze, die nachfolgend beschrieben werden.

Fall 1: $\mathrm{DIFS_A}$=$\mathrm{DIFS_B}$

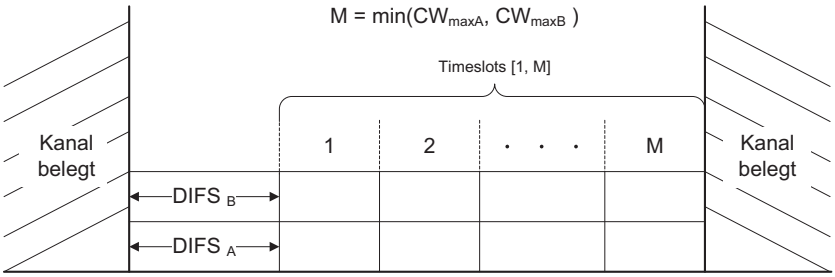


Abbildung 5.5: Verteilung der Zeitschlitze für den Fall $DIFS_A = DIFS_B$

Für den Fall, dass $\mathrm{DIFS_A}$=$\mathrm{DIFS_B}$ ist, ergibt sich eine Verteilung der Zeitschlitze wie in Abbildung 5.5. In diesem Fall können Nutzer den *Backoff Prozess* nach einem *Idle Slot* starten. Somit ist für jeden Zeitschlitz eines der folgenden Ereignisse möglich:

1. Übertragung von $\mathrm{AC_A}$ und keine Übertragung von $\mathrm{AC_B}$.

2. Übertragung von AC_B und keine Übertragung von AC_A.
3. Gleichzeitige Übertragung von AC_A und AC_B.
4. Keine Übertragung sowohl von AC_A als auch von AC_B.

Fall 2: $DIFS_A < DIFS_B$

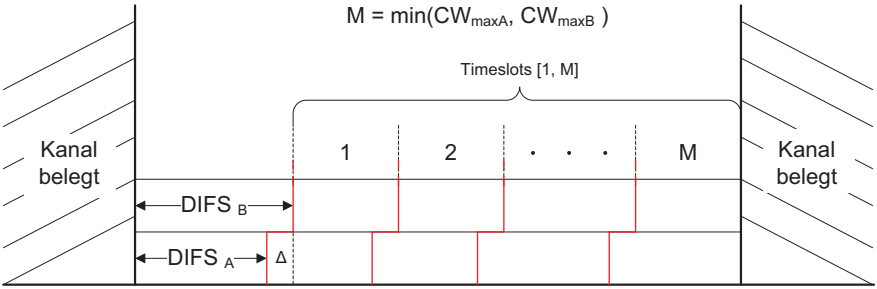


Abbildung 5.6: Verteilung der Zeitschlitze für den Fall $DIFS_A < DIFS_B$

Im Vergleich zum ersten Fall treten die folgenden Unterschiede auf: Nach einem *Idle Slot* können zunächst Nutzer der Kategorie AC_A ihre Backoff-Prozedur starten. Nach einer zusätzlichen kurzen Periode Δ_{DIFS} können auch Nutzer der Kategorie AC_B ihre Backoff-Prozedur starten. Der zweite Unterschied besteht darin, dass entweder ein AC_A- oder ein AC_B-Nutzer eine Übertragung starten kann. Der Grund dafür ist die zusätzliche Wartezeit von Δ_{DIFS}. All dies führt dazu, dass drei unterschiedliche Fälle pro Zeitschlitz untersucht werden müssen. Darüber hinaus werden zusätzliche Zustände in der Markov-Kette benötigt, welche die kurze Wartezeit Δ_{DIFS} repräsentieren.

1. Übertragung von AC_A und keine Übertragung von AC_B.
2. Übertragung von AC_B und keine Übertragung von AC_A.
3. Keine Übertragung von sowohl AC_A als auch von AC_B.

Ziel des analytischen Modells

Ziel des hier vorgestellten analytischen Modells ist die Berechnung des Durchsatzes im Wettbewerb von jeweils zwei Zugriffskategorien. Die errechneten Durchsätze werden miteinander verglichen und ermöglichen damit Rückschlüsse auf die Effektivität der Priorisierung. Wesentlich hierfür sind die beiden nachfolgend vorgestellten Markov-Ketten-Modelle. Das erste Modell wird verwendet, wenn für

beide konkurrierenden Zugriffskategorien AC_A und AC_B die gleiche SIFS-Dauer definiert ist (siehe Tabelle 5.2). Da die SIFS-Dauer direkt mit der DIFS-Dauer verknüpft ist, unterliegen die Markov-Ketten-Modelle für AC_A und AC_B den beiden oben beschriebenen Möglichkeiten. Für den Fall, dass $DIFS_A = DIFS_B$ ist, werden beide Nutzer von dem Markov-Ketten-Modell repräsentiert, welches in Abbildung 5.7 dargestellt ist. Falls $DIFS_A < DIFS_B$ ist, müssen zwei Markov-Ketten-Modelle betrachtet werden. Das Modell für den Nutzer der AC_A ist in Abbildung 5.7 dargestellt, und das Modell für den Nutzer der AC_B wird in Abbildung 5.9 aufgezeigt.

Beide Markov-Ketten-Modelle basieren auf zwei stochastischen Prozessen. Der erste Prozess $w(t)$ stellt das Herunterzählen des Backoff Zählers dar. Der Zustand $w(t) = -1$ gibt den Übertragungsversuch an. Der zweite Prozess $v(t)$ repräsentiert das Pausieren des *Backoffs*, welches aus drei Zuständen besteht:

- $v(t) = 0 \rightarrow$ Normaler Backoff-Prozess oder Übertragungszustand.
- $v(t) = \Delta_{DIFS} \rightarrow$ Zustand der anzeigt, dass die Dauer Δ_{DIFS} nach $DIFS_A$ vorüber ist. Daher können Nutzer der AC_B den Backoff-Prozess zwischen $DIFS_A$ und dem normalen Backoff starten.
- $v(t) = -1 \rightarrow$ Ein anderer Nutzer überträgt Daten.

5.5.3 Markov-Kette für AC_A

Zunächst wird das Markov-Ketten-Modell für die Zugriffskategorie AC_A in Abbildung 5.7 vorgestellt. Die Nomenklatur des hier hergeleiteten mathematischen Modells orientiert sich an der Nomenklatur des Modells der EDCA von *Xiong* aus [104]. Die Markov-Kette besteht aus Zuständen $Z(w(t), v(t))$ und Zustandsübergängen. Die Zustandsübergänge sind mit ihrer Übergangswahrscheinlichkeit gekennzeichnet. Die Zustände sind in zwei Zeilen angeordnet. In der unteren Zeile befinden sich die Zustände, welche den gewöhnlichen *Backoff* der Station modellieren. Die obere Zeile modelliert die Belegung des Kanals durch eine andere Station, also den *Backoff freeze*.

Der Zustand $Z(-1, 0)$ repräsentiert den Übertragungsversuch der Station. Der Übergang in den darauf folgenden Zustand hängt von zwei Wahrscheinlichkeiten ab, nämlich der Wahrscheinlichkeit, dass der Kanal durch eine andere Station belegt ist (P_{bA}), und der Wahrscheinlichkeit, dass die betrachtete Station eine Backoff-Prozedur mit dem Startwert r startet ($Pr_{A(r)}$). Die Wahrscheinlichkeit $Pr_{A(r)}$ berücksichtigt indirekt den *Backoff-Stage*, also die Anzahl der erfolglosen aufeinander folgenden Übertragungsversuche und die damit verbundene Vergrößerung des Wettbewerbsfensters. Dies führt dazu, dass große Werte für r seltener gezogen werden, als kleinere. Dieser Zusammenhang wird in Kapitel 5.5.5 näher beschrieben.

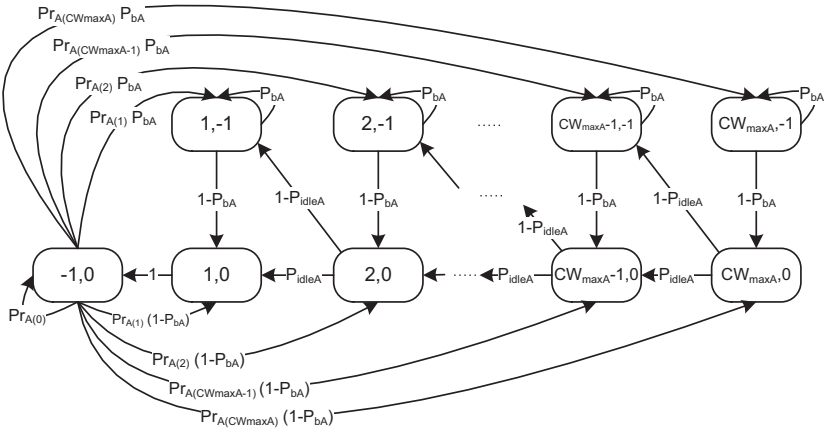


Abbildung 5.7: Markov-Ketten Modell für AC_A (im Falle $DIFS_A < DIFS_B$) oder für AC_A und AC_B (im Falle $DIFS_A = DIFS_B$)

Während der normalen *Backoff Prozedur* können zwei Fälle eintreten. Entweder der Kanal ist frei (P_{idleA}), oder eine andere Station greift auf den Kanal zu (1-P_{idleA}). Wenn der Kanal frei ist, dann wechselt die Station vom Zustand $Z(r,0)$ nach $Z(r-1,0)$. Wenn der Kanal durch eine andere Station belegt wird, dann wechselt die Station vom Zustand $Z(r,0)$ nach $Z(r-1,-1)$.

Wenn im vorherigen Zustand eine andere Station den Kanal belegt hat, dann befindet sich die Station im Zustand $Z(r,-1)$, also in einem Zustand in der oberen Zeile der Markov-Kette. Wenn der Kanal belegt bleibt (P_{bA}), dann bleibt die Station in dem Zustand $Z(r,-1)$. Wird der Kanal frei (1-P_{bA}), dann wechselt die Station in den Zustand $Z(r,0)$.

Aus dem Modell in Abbildung 5.7 können direkt die Gleichungen zur Bestimmung der stationären Zustände abgelesen werden. Zuerst werden die Übergangswahrscheinlichkeiten für die Zustandsübergänge vom Zustand *Z(-1,0)* abgelesen. Dieser Zustand ist in Abbildung 5.7 unten links dargestellt. Bei der Betrachtung dieses Zustands fällt auf, dass die Zustandsübergänge in drei Fälle eingeteilt werden können. Zustandsübergänge, die oben aus *Z(-1,0)* abgehen, können unter der Übergangswahrscheinlichkeit $P\{(r,-1)|(-1,0))\}$, mit $r \in \{1 \ldots CW_{maxA}\}$, zusammengefasst werden. Darüber hinaus lassen sich die Zustandsübergänge, die unten aus *Z(-1,0)* abgehen mit $P\{(r,0)|(-1,0))\}$, mit $r \in \{1 \ldots CW_{maxA}\}$ zusammenfassen. Schließlich kann die Übergangswahrscheinlichkeit des Zustandsübergangs von *Z(-1,0)* in *Z(-1,0)*, also der Verbleib im Ausgangszustand, mit $P\{(-1,0)|(-1,0))\}$

angegeben werden. So ergeben sich die folgenden drei Fälle für die Übergangswahrscheinlichkeiten.

$$\begin{cases} P\{(r,0)|(-1,0)\} = Pr_A(r) \cdot (1 - P_{bA}) \\ P\{(r,-1)|(-1,0)\} = Pr_A(r) \cdot P_{bA} \\ P\{(-1,0)|(-1,0)\} = Pr_A(0) \end{cases} \tag{5.4}$$

Mit den folgenden drei Übergangswahrscheinlichkeiten können die Zustandsübergänge aus den Zuständen *Z(r,0)* mit $r \in \{1 \ldots CW_{maxA}\}$, beschrieben werden. Diese Zustände befinden sich auf der unteren Reihe in Abbildung 5.7.

$$\begin{cases} P\{(r-1,0)|(r,0)\} = P_{idleA} \\ P\{(r-1,-1)|(r,0)\} = 1 - P_{idleA} \\ P\{(-1,0)|(1,0)\} = 1 \end{cases} \tag{5.5}$$

Bei der oberen Reihe der Zustände, *Z(r,-1)* mit $r \in \{1 \ldots CW_{maxA}\}$, können die Übergänge mit zwei Gleichungen beschrieben werden.

$$\begin{cases} P\{(r,0)|(r,-1)\} = 1 - P_{bA} \\ P\{(r,-1)|(r,-1)\} = P_{bA} \end{cases} \tag{5.6}$$

Nachdem alle Zustandsübergänge des Markov-Ketten-Modells mathematisch beschrieben sind, kann das Gleichungssystem für die stationären Zustandswahrscheinlichkeiten $b_{A(r,k)}$ der Zustände (r,k) angegeben werden. Die stationäre Zustandswahrscheinlichkeit $b_{A(r,k)}$ eines Zustands Z kann durch die Gleichgewichtsbedingung ermittelt werden.

Um die Gleichungen nachvollziehbar darzustellen, sind in Abbildung 5.8 die Zustände zu den korrespondierenden Gleichungen markiert. Dabei sind Zustände zusammengefasst, die in Bezug auf die eingehenden und abgehenden Zustandsübergänge ähnlich sind. In Abbildung 5.8 sind diese Zusammenfassungen durch schwarze Umrandungen markiert.

Die stationäre Zustandswahrscheinlichkeit $b_{A(CW_{maxA},0)}$ wird in Gleichung 5.7 für den Zustand $Z(CW_{maxA},0)$ angegeben. In der Gleichung taucht P_{idleA} nicht auf, da die beiden ausgehenden Zustandsübergänge von $b_{A(CW_{maxA},0)}$ aufsummiert $(P_{idleA} + (1 - P_{idleA}))$ 1 ergeben. Dies bedeutet, dass der Zustand auf jeden Fall verlassen wird.

$$b_{A(CW_{maxA},0)} = (1 - P_{bA}) \cdot (b_{A(-1,0)} \cdot Pr_{A(CW_{maxA})} + b_{A(CW_{maxA},-1)}) \tag{5.7}$$

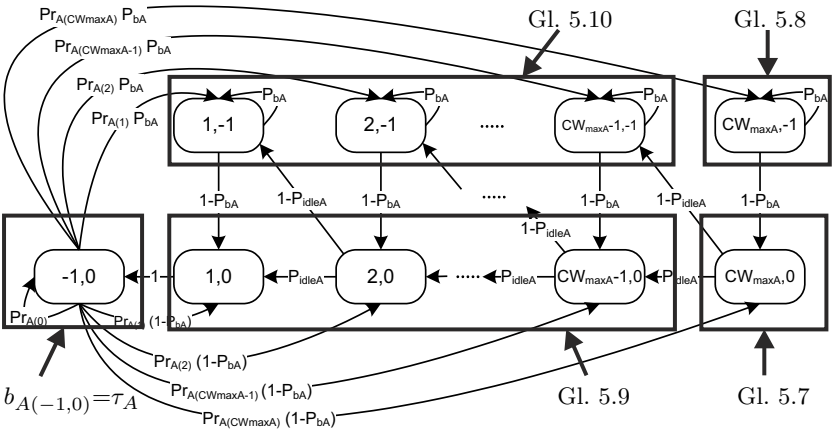


Abbildung 5.8: Markierte Zustände im Markov Modell für AC_A mit korrespondierenden Gleichungen

Die stationäre Zustandswahrscheinlichkeit $b_{A(CW_{maxA},-1)}$ wird in Gleichung 5.8 für den Zustand $Z(CW_{maxA},-1)$ angegeben.

$$b_{A(CW_{maxA},-1)} = \frac{b_{A(-1,0)} \cdot Pr_{A(CW_{maxA})} \cdot P_{bA}}{1 - P_{bA}} \tag{5.8}$$

Die stationäre Zustandswahrscheinlichkeit $b_{A(r,0)}$ für die Zustände $Z(r,0)$, mit $r \in \{1 \ldots CW_{maxA} - 1\}$, lässt sich durch die Gleichung 5.9 zusammenfassen, da in diesem Bereich für r dieselben Zustandsübergänge ein- und ausgehen. Bei dem Zustand $Z(1,0)$ geht nur ein Übergang mit der Übergangswahrscheinlichkeit 1 ab, was aber dem Übergang der übrigen Zustände $Z(r,0)$ mit $r \geq 2$ mit $P_{idle} + (1 - P_{idle}) = 1$ entspricht.

$$b_{A(r,0)} = (1 - P_{bA}) \cdot (b_{A(-1,0)} \cdot Pr_{A(r)} + b_{A(r,-1)}) + b_{A(r+1,0)} \cdot P_{idleA} \tag{5.9}$$

Eine ähnliche Zusammenfassung kann für die stationäre Zustandswahrscheinlichkeit der Zustände $Z(r,-1)$, mit $r \in \{1 \ldots CW_{maxA} - 1\}$, durch $b_{A(r,-1)}$ in Gleichung 5.10 angeben werden.

$$b_{A(r,-1)} = \frac{b_{A(-1,0)} \cdot Pr_{A(r)} \cdot P_{bA} + b_{A(r+1,0)} \cdot (1 - P_{idleA})}{1 - P_{bA}} \tag{5.10}$$

Zusätzlich besagt die Gleichgewichtsbedingung der Markov-Kette, dass die Summe aller stationären Zustandswahrscheinlichkeiten $= 1$ ist.

$$\sum b_{A(r,k)} = 1 \tag{5.11}$$

Da der Zustand $Z(-1,0)$ den Übertragungsprozess der Station repräsentiert, wird die entsprechende stationäre Zustandswahrscheinlichkeit $b_{A(-1,0)}$ gleich der Übertragungswahrscheinlichkeit τ_A gewählt (siehe Abbildung 5.8), wobei τ_A die unbekannte Übertragungswahrscheinlichkeit für die Durchsatzberechnung ist.

5.5.4 Markov-Kette für AC_B, wenn $DIFS_A < DIFS_B$

Nachfolgend wird das Markov-Ketten Modell für die Zugriffskategorie AC_B in Abbildung 5.9 vorgestellt. Die Zustände $Z(r,0)$, mit $r \in \{1 \ldots CW_{maxB}\}$, in der mittleren Reihe und die Zustände $Z(r,-1)$ entsprechen den Zuständen aus der zuvor beschriebenen Markov-Kette für den Fall $DIFS_A = DIFS_B$.

Neu hinzugekommen sind die Zustände, welche durch den Unterschied in den SIFS-Parametern der AC_A und AC_B entstehen. Nachdem der Kanal belegt war, muss Station B zunächst in den Wartezustand $Z(r,\Delta)$ wechseln. Dies repräsentiert die Priorisierung der Station A gegenüber der Station B, wenn beide Stationen den gleichen Backoff-Zähler gezogen hätten.

Die zusätzlichen Zustände führen auch zu neuen Zustandsübergängen. Befindet sich die Station im Zustand $Z(r,-1)$, so bleibt sie weiterhin in dem Zustand, solange der Kanal mit der Übergangswahrscheinlichkeit P_{sB} belegt bleibt. Wird der Kanal mit der Übergangswahrscheinlichkeit $(1-P_{sB})$ frei, so wechselt die Station in den Zustand $Z(r,\Delta)$.

Im Zustand $Z(r,\Delta)$ befindet sich die Station nur sehr kurz. Wenn in der Zwischenzeit Station A nicht auf den Kanal zugegriffen hat, also der Kanal weiterhin frei ist (1-P_{bB}), dann wechselt die Station B in den Zustand $Z(r,0)$. Belegt Station A den Kanal (P_{bB}), so wechselt Station B wieder in den Zustand $Z(r,-1)$.

Aus der Markov-Kette in Abbildung 5.9 können die Gleichungen zur Bestimmung der stationären Zustände abgelesen werden. Für den Zustand $Z(-1,0)$, der sich in Abbildung 5.9 unten links befindet, können die Übergangswahrscheinlichkeiten für zwei Zustandsübergänge wie folgt angegeben werden.

$$\begin{cases} P\{(-1,\Delta)|(-1,0)\} = 1 - P_{sB} \\ P\{(-1,-1)|(-1,0)\} = P_{sB} \end{cases} \tag{5.12}$$

Vom Zustand $Z(-1,\Delta)$ gehen drei unterschiedliche Arten von Zustandsübergängen aus. Der Zustand $Z(-1,\Delta)$ befindet sich links oben in der Abbildung.

$$\begin{cases} P\{(r,0)|(-1,\Delta)\} = Pr_B(r) \cdot (1 - P_{bB}) \\ P\{(r,-1)|(-1,\Delta)\} = Pr_B(r) \cdot P_{bB} \\ P\{(-1,0)|(-1,\Delta)\} = Pr_B(0) \end{cases} \tag{5.13}$$

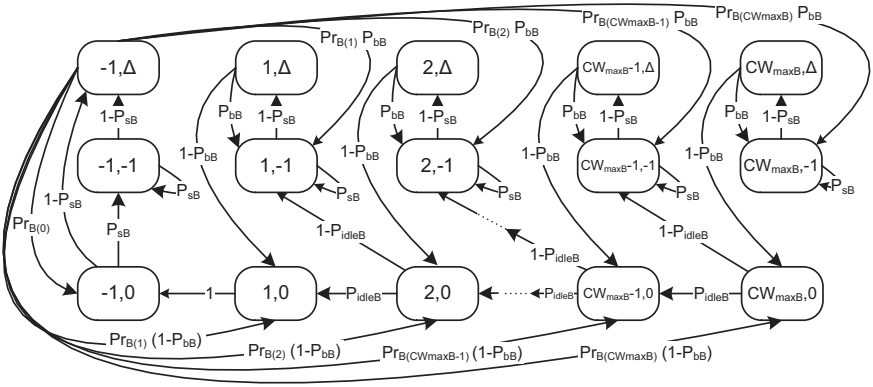


Abbildung 5.9: Markov-Ketten Modell für $\mathrm{AC_B}$ (im Falle $DIFS_A < DIFS_B$)

Für die Zustände, *Z(r,0)* mit $r \in \{2 \ldots CW_{maxB}\}$, die sich in der mittleren Reihe der Abbildung 5.9 befinden, werden die folgenden Zustandsübergänge abgelesen.

$$\begin{cases} P\{(r-1,0)|(r,0)\} = P_{idleB} \\ P\{(r-1,-1)|(r,0)\} = 1 - P_{idleB} \end{cases} \tag{5.14}$$

Für den Zustand *Z(1,0)* kann folgender Zustandsübergang abgelesen werden:

$$P\{(-1,0)|(1,0)\} = 1 \tag{5.15}$$

Die Zustandsübergänge der Zustände *Z(r,-1)* mit $r \in \{-1 \ldots CW_{maxB}\}$, die sich in der zweiten Reihe von oben in der Abbildung 5.9 befinden, können wie folgt abgelesen werden.

$$\begin{cases} P\{(r,\Delta)|(r,-1)\} = 1 - P_{sB} \\ P\{(r,-1)|(r,-1)\} = P_{sB} \end{cases} \tag{5.16}$$

Für die noch fehlenden Zustände in der oberen Reihen in Abbildung 5.9, *Z(r,Δ)* mit $r \in \{1 \ldots CW_{maxB}\}$, können die folgenden Zustandsübergänge abgelesen werden:

$$\begin{cases} P\{(r,0)|(r,\Delta)\} = 1 - P_{bB} \\ P\{(r,-1)|(r,\Delta)\} = P_{bB} \end{cases} \tag{5.17}$$

Mit den Zustandsübergängen des Markov-Ketten-Modells aus Abbildung 5.9 kann das Gleichungssystem für die stationären Zustandswahrscheinlichkeiten $b_{B(r,k)}$ der Zustände (r,k) angegeben werden. Um die folgenden Gleichungen für die statio-

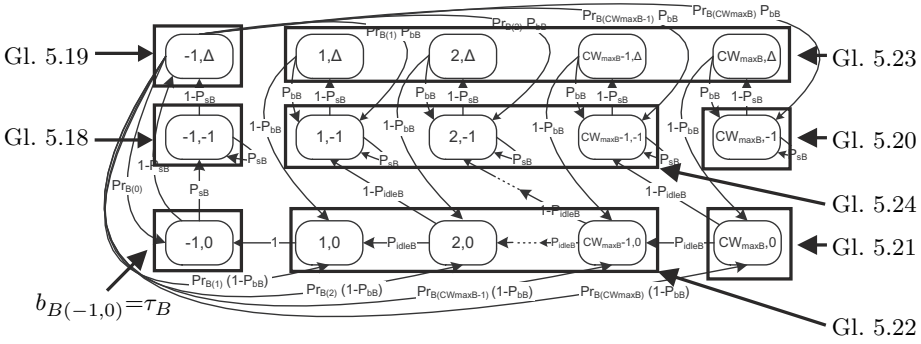


Abbildung 5.10: Markierte Zustände im Markov Modell für AC_B mit korrespondierenden Gleichungen

nären Zustandswahrscheinlichkeiten $b_{B(r,k)}$ nachvollziehbar darzustellen, werden in Abbildung 5.10 die Zustände zu den korrespondierenden Gleichungen markiert. Dabei sind Zustände zusammengefasst, die in Bezug auf die eingehenden und abgehenden Zustandsübergänge ähnlich sind. In Abbildung 5.10 sind die folgenden Zusammenfassungen mit einem Rahmen markiert.

Zunächst werden in den Gleichungen 5.18 bis 5.21 die stationären Zustandswahrscheinlichkeiten für die Zustände berechnet, die sich nicht zusammenfassen lassen. In Gleichung 5.18 wird die stationäre Zustandswahrscheinlichkeit für den Zustand $Z(-1,-1)$ angegeben. Der Übergang P_{sB} kann vernachlässigt werden, da er in den gleichen Zustand $Z(-1,-1)$ führt.

$$b_{B(-1,-1)} = \frac{b_{B(-1,0)} \cdot P_{sB}}{1 - P_{sB}} \tag{5.18}$$

In Gleichung 5.19 wird die stationäre Zustandswahrscheinlichkeit für den Zustand $Z(-1,\Delta)$ angegeben. Da dieser Zustand zum nächsten Timeslot verlassen wird, ist die Summe der ausgehenden Übergänge gleich 1.

$$b_{B(-1,\Delta)} = (b_{B(-1,0)} + b_{B(-1,-1)}) \cdot (1 - P_{sB}) \tag{5.19}$$

Die stationäre Zustandswahrscheinlichkeit für den Zustand $Z(CW_{maxB},-1))$ wird in Gleichung 5.20 angegeben.

$$b_{B(CW_{maxB},-1)} = \frac{P_{bB} \cdot Pr_{B(CW_{maxB})} \cdot (b_{B(-1,\Delta)} + b_{B(CW_{maxB},\Delta)})}{1 - P_{sB}} \tag{5.20}$$

Die stationäre Zustandswahrscheinlichkeit für den Zustand $Z(CW_{maxB},0)$ wird in Gleichung 5.21 angegeben. Die Summe der ausgehenden Übergänge $P_{idleB} + (1-P_{idleB}) = 1$ kann auf der linken Seite der Gleichung vernachlässigt werden.

$$b_{B(CW_{maxB},0)} = (1-P_{bB}) \cdot Pr_{B(CW_{maxB})} \cdot (b_{B(-1,\Delta)} + b_{B(CW_{maxB},\Delta)}) \quad (5.21)$$

In Gleichung 5.22 wird die stationäre Zustandswahrscheinlichkeit für die Zustände $Z(r,0)$, mit $r \in \{1 \ldots CW_{maxB-1}\}$, angegeben. Von dem Zustand $Z(1,0)$ geht zwar nur ein Übergang ab, aber die zugehörige Übergangswahrscheinlichkeit 1 entspricht der Summe $P_{idleB} + (1-P_{idleB}) = 1$. Daher wird die stationäre Zustandswahrscheinlichkeit des Zustands $Z(1,0)$ auch durch die Gleichung 5.22 repräsentiert.

$$b_{B(r,0)} = (1-P_{bB})(Pr_{B(r)} \cdot b_{B(-1,\Delta)} + b_{B(r,\Delta)}) + P_{idleB} \cdot b_{B(r+1,0)} \quad (5.22)$$

In Gleichung 5.23 wird die stationäre Zustandswahrscheinlichkeit für die Zustände $Z(r,\Delta)$, mit $r \in \{1 \ldots CW_{maxB}\}$, angegeben. Die Summe der abgehenden Übergangswahrscheinlichkeiten ist eins.

$$b_{B(r,\Delta)} = (1-P_{sB}) \cdot b_{B(r,-1)} \quad (5.23)$$

In Gleichung 5.24 wird die stationäre Zustandswahrscheinlichkeit für die Zustände $Z(r,-1)$, mit $r \in \{1 \ldots CW_{maxB-1}\}$, angegeben.

$$b_{B(r,-1)} = \frac{P_{bB} \cdot (Pr_{B(r)} \cdot b_{B(-1,\Delta)} + b_{B(r,\Delta)}) + (1-P_{idleB}) \cdot b_{B(r+1,0)}}{1-P_{sB}} \quad (5.24)$$

Es gilt zusätzlich die Gleichgewichtsbedingung der Markov-Kette, die besagt, dass die Summe aller stationären Zustandswahrscheinlichkeiten $= 1$ ist.

$$\sum b_{B(r,k)} = 1 \quad (5.25)$$

Die entsprechende stationäre Zustandswahrscheinlichkeit $b_{B(-1,0)}$ soll gleich der Übertragungswahrscheinlichkeit τ_B sein, wobei τ_B die unbekannte, gesuchte Übertragungswahrscheinlichkeit ist.

5.5.5 Berechnung der unbekannten Zustandsübergänge

Für die Berechnung der unbekannten Zustandsübergänge wird eine Kombination aus beiden Markov-Systemen betrachtet, wobei eine Anzahl n_a Nutzer des Systems A gegen eine Anzahl n_b des Systems B um den Kanalzugriff wetteifern. Von besonderem Interesse ist hierbei die Wahrscheinlichkeit für eine Kollision p. Diese Kollisionswahrscheinlichkeit wird anschließend genutzt, um die Startwerte des *Backoff*-Zählers $Pr_{A(r)}$ bzw. $Pr_{B(r)}$ zu berechnen. Wenn die Gleichungen aller Zustandsübergänge bekannt sind, kann im Anschluss der Durchsatz der EDCF berechnet werden. Um am Ende des Abschnitts die beiden Parameter $Pr_{A(r)}$ und

$Pr_{B(r)}$ bestimmen zu können, müssen die beiden Fälle $\mathrm{DIFS_A} = \mathrm{DIFS_B}$ und $\mathrm{DIFS_A} < \mathrm{DIFS_B}$ getrennt voneinander betrachtet werden.

Systemparameter für den Fall $\mathrm{DIFS_A} = \mathrm{DIFS_B}$

Wenn $\mathrm{DIFS_A} = \mathrm{DIFS_B}$, dann wird das Modell der Markov-Kette aus Abbildung 5.7 zur Berechnung der Systemparameter verwendet. Daraus ergeben sich folgende Systemparameter:

$\mathrm{P_{idleA}}$ bzw. $\mathrm{P_{idleB}}$: Wahrscheinlichkeit, dass der Kanal frei bleibt, also kein anderer Nutzer eine Übertragung durchführt.

$$\begin{cases} P_{idleA} = (1-\tau_A)^{n_A-1} \cdot (1-\tau_B)^{n_B} \\ P_{idleB} = (1-\tau_B)^{n_B-1} \cdot (1-\tau_A)^{n_A} \end{cases} \tag{5.26}$$

$\mathrm{P_{bA}}$ bzw. $\mathrm{P_{bB}}$: Wahrscheinlichkeit, dass mindestens ein anderer Nutzer auf den Kanal zugreift bzw. eine Übertragung startet. Dabei wird die eigene *Backoff*-Prozedur pausiert. Dies ist das komplementäre Ereignis zu P_{idleA} bzw. P_{idleB}. In der Wahrscheinlichkeitstheorie wird es auch Gegenereignis genannt und ist wie folgt definiert: $P(\overline{A}) = 1 - P(A)$.

$$\begin{cases} P_{bA} = 1 - P_{idleA} \\ P_{bB} = 1 - P_{idleB} \end{cases} \tag{5.27}$$

p_A bzw. p_B: Kollisionswahrscheinlichkeit. Wenn mindestens ein weiterer Nutzer gleichzeitig mit der Übertragung startet, dann kommt es zur Kollision. Die Berechnung der Kollisionswahrscheinlichkeit erfolgt auf die gleiche Weise wie die Berechnung für die Wahrscheinlichkeit, dass ein anderer Nutzer auf den Kanal zugreift. Der Unterschied besteht lediglich darin, dass der betrachtete Nutzer sich nicht mehr in der Backoff-Prozedur befindet, sondern gerade in den Übertragungszustand gewechselt ist.

$$\begin{cases} p_A = P_{bA} \\ p_B = P_{bB} \end{cases} \tag{5.28}$$

Systemparameter für den Fall $\mathrm{DIFS_A} < \mathrm{DIFS_B}$

Wenn $\mathrm{DIFS_A} < \mathrm{DIFS_B}$, dann wird das Modell der Markov-Kette aus Abbildung 5.9 zur Berechnung der Systemparameter verwendet. Die Systemparameter ergeben sich daraus wie folgt:

$\mathrm{P_{idleA}}$ bzw. $\mathrm{P_{idleB}}$: Die Wahrscheinlichkeit, dass der Kanal frei bleibt, ist genauso definiert wie im ersten Fall (siehe Gleichung 5.26 weiter oben).

P_{bA} bzw. P_{bB}: Wahrscheinlichkeit, dass mindestens ein anderer Nutzer auf den Kanal zugreift bzw. eine Übertragung startet. Aufgrund der unterschiedlichen DIFS-Zeiten müssen nicht mehr beide Zugriffskategorien berücksichtigt werden. Somit ergibt sich die Wahrscheinlichkeit wie folgt:

$$\begin{cases} P_{bA} = 1-(1-\tau_A)^{n_A-1} \\ P_{bB} = 1-(1-\tau_B)^{n_B-1} \end{cases} \tag{5.29}$$

p_A bzw. p_B: Kollisionswahrscheinlichkeit. Bei der Bestimmung der Kollisionswahrscheinlichkeit muss berücksichtigt werden, dass eine Kollision nur bei gleichzeitiger Übertragung mindestens eines Nutzers derselben Zugriffskategorie stattfindet. Dabei überträgt zeitgleich kein Nutzer aus einer anderen Zugriffskategorie. Somit ergibt sich für die Kollisionswahrscheinlichkeit folgende Gleichung:

$$\begin{cases} p_A = (1-\tau_B)^{n_B} \cdot \left[1-(1-\tau_A)^{n_A-1}\right] \\ p_B = (1-\tau_A)^{n_A} \cdot \left[1-(1-\tau_B)^{n_B-1}\right] \end{cases} \tag{5.30}$$

P_{sB}: Wahrscheinlichkeit, dass während $DIFS_B$ mindestens ein anderer Nutzer der Kategorie AC_A auf den Kanal zugreift. Diese Wahrscheinlichkeit kommt nur bei der AC_B vor und entsteht aufgrund der unterschiedlichen DIFS von AC_A und AC_B.

$$P_{sB} = 1-(1-\tau_A)^{n_A} \tag{5.31}$$

Systemparameter $Pr_{A(r)}$ und $Pr_{B(r)}$

Für die Modellierung des Zählers für den Backoff-Prozess in Abhängigkeit von den zuvor gescheiterten Übertragungen werden die Systemparameter $Pr_{A(r)}$ und $Pr_{B(r)}$ verwendet. Die Modellierung ist unabhängig von der oben genannten Fallunterscheidung. Bei der klassischen Modellierung der DCF nach *Bianchi* [5] wird jeder *Backoff-Stage* einzeln modelliert. Bei dem hier vorgestellten Vorgehen, dass sich an [104] orientiert, wird der *Backoff-Stage* in den Systemparametern $Pr_{A(r)}$ und $Pr_{B(r)}$ direkt berücksichtigt.

Die Vergrößerung des Wettbewerbsfensters nach einer Kollision, bis zum Erreichen des Wertes CW_{max} , wird durch eine Gewichtung mit der Wahrscheinlichkeit des *Backoff-Stages* bei der Berechnung von $Pr_{A(r)}$ und $Pr_{B(r)}$ modelliert. Diese Wahrscheinlichkeit wird durch die in Abbildung 5.11 dargestellte Markov-Kette bestimmt. Hierbei modelliert die Markov-Kette die *Backoff-Stages*. Eine Wiederholung findet statt, wenn eine Kollision mit einer Wahrscheinlichkeit von p_A bzw. p_B auftritt.

In Abbildung 5.11 repräsentiert der Parameter p die beiden Systemparameter p_A und p_B, und jeder Zustand einen *Backoff-Stage*. Der Zustand h repräsentiert den

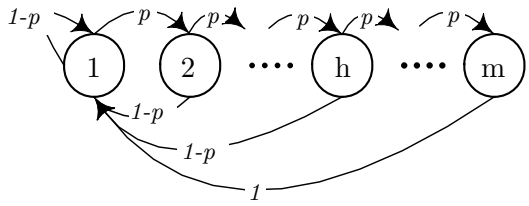


Abbildung 5.11: Markov-Kette zur Modellierung der *Backoff-Stages*

Backoff-Stage, bei dem CW_{max} zum ersten Mal erreicht wird. In den folgenden *Backoff-Stages* wird das Wettbewerbsfenster nicht mehr vergrößert. Nach dem letzten *Backoff-Stage* m wird das aktuelle Paket entweder erfolgreich übertragen oder aber verworfen. Die nächste Übertragung startet auf jeden Fall wieder im *Backoff-Stage* 1. In der Regel ist der Zustand $h = m$.

Im Folgenden wird die stationäre Zustandswahrscheinlichkeit für den Zustand k, mit $k \in \{1 \dots m\}$, gesucht, die den *k-ten Backoff-Stage*, bzw. den *k-ten* aufeinander folgenden Übertragungsversuch, repräsentiert.

Wenn der *k-te* Übertragungsversuch fehlschlägt, wechselt das System mit der Wahrscheinlichkeit p vom Zustand k zum Zustand $k+1$, wobei p die AC-spezifische durchschnittliche Kollisionswahrscheinlichkeit ist, die aus Gleichung 5.30 berechnet werden kann.

$$P\{(k+1)|(k)\} = p, \text{ für } 1 \leq k \leq m-1. \tag{5.32}$$

Wenn der *k-te* Kanalzugriff erfolgreich ist, wechselt das System mit der Wahrscheinlichkeit $1-p$ vom Zustand k zum Zustand 1, und die Station wird mit der Übertragung beginnen.

$$P\{(1)|(k)\} = 1-p, \text{ für } 1 \leq k \leq m. \tag{5.33}$$

Wenn die maximale Anzahl m an Übertragungsversuchen erreicht ist, wird die Station im nächsten Zustand eine neue Übertragung starten, unabhängig davon, ob das aktuelle Daten-Frame erfolgreich übertragen werden konnte. Daher wird das System mit der Wahrscheinlichkeit 1 zum Zustand 1 zurückkehren.

$$P\{(1)|(m)\} = 1. \tag{5.34}$$

Mittels Gleichung 5.32 kann die Beziehung zweier aufeinander folgender Zustände in Gleichung 5.35 angegeben werden, wobei $d_{(k)}$ die korrespondierende stationäre Zustandswahrscheinlichkeit für den Zustand k ist.

$$d_{(k+1)} = d_{(k)}p. \tag{5.35}$$

Aufgrund der Gleichgewichtsbedingung der Markov-Kette ist die Summe aller stationären Zustandswahrscheinlichkeiten 1.

$$\sum_{k=1}^{m} d_{(k)} = 1. \tag{5.36}$$

Damit kann die stationäre Zustandswahrscheinlichkeit $d(k)$ in Gleichung 5.37 angegeben werden.

$$d_{(k)} = \frac{p^{k-1}(1-p)}{1-p^m}, \text{ für } 1 \leq k \leq m. \tag{5.37}$$

Da der Backoff-Zähler bei einer Zufallszahl startet, die gleichverteilt aus dem Wertebereich $\{0 \cdots CW\}$ gezogen wird, ist die Wahrscheinlichkeit, einen spezifischen Backoff-Zähler aus diesem Bereich zu ziehen, $\frac{1}{1+CW}$. Somit kann die AC-spezifische Wahrscheinlichkeit $Pr(r)$ für das Ziehen eines Backoff-Zählers r durch die Summe der Wahrscheinlichkeiten für das Ziehen dieses Backoff-Zählers r im $k-ten$ aufeinander folgenden Übertragungsversuch, gewichtet mit der Wahrscheinlichkeit des Auftretens des k-*ten* aufeinander folgenden Übertragungsversuchs, ausgedrückt werden.

$$Pr(r) = \sum_{k=1}^{m} \frac{d_{(k)} c_{(r)}}{CW(k)+1}. \tag{5.38}$$

In Gleichung 5.38 steht $d_{(k)}$ für die stationäre Zustandswahrscheinlichkeit für den k-*ten* aufeinander folgenden Übertragungsversuch, die durch die Gleichung 5.37 berechnet werden kann. $CW(k)$ ist die korrespondierende Größe des Wettbewerbsfensters beim k-*ten* aufeinander folgenden Übertragungsversuch. $c_{(r)}$ zeigt an, ob sich der spezifische Wert r innerhalb des erlaubten Wertebereichs $\{0 \ldots CW(k)\}$ befindet. Wenn sich der Wert r innerhalb des Bereichs befindet, dann ist $c_{(r)} = 1$, sonst ist er null.

Daraus ergeben sich für $Pr(r)$ drei unterschiedliche Fälle, die davon abhängen, in welchem Wertebereich r sich befindet. Der Bereich $r \in \{0 \ldots CW_{min}\}$ ist am wahrscheinlichsten, da dieser Bereich von dem ersten *Backoff-Stage* an möglich ist. Somit ergibt sich folgende Wahrscheinlichkeit, wobei die zweite Summe daraus resultiert, dass sich ab dem *Backoff-Stage* h bis zum *Backoff-Stage* m der Wert für $\mathrm{CW}_{\max}$ nicht mehr ändert.

$$Pr(r) = \sum_{k=1}^{h-1} \frac{d(k)}{2^{k-1}CW_{min}+1} + \sum_{k=h}^{m} \frac{d(k)}{CW_{max}+1} \quad \text{für } 0 \leq r \leq CW_{min} \tag{5.39}$$

Die Wahrscheinlichkeiten im Wertebereich $r \in \{CW_{min}+1 \ldots 2^{h-1}CW_{min}\}$ hängen davon ab, wo sich r in dem Bereich befindet, da höhere r-Werte nur in höheren *Backoff-Stages* erreicht werden. Die Abhängigkeit vom *Backoff-Stage* wird in Gleichung 5.40 durch j ausgedrückt.

$$Pr(r) = \sum_{k=j}^{h-1} \frac{d(k)}{2^{k}CW_{min}+1} + \sum_{k=h}^{m} \frac{d(k)}{CW_{max}+1} \quad \text{für } 2^{j-1}CW_{min}+1 \leq r \leq 2^{j}CW_{min} \text{ und } 1 \leq j \leq h-1 \tag{5.40}$$

Der letzte Wertebereich $r \in \{2^{h-1}CW_{min}+1 \ldots CW_{\max}\}$ wird nur in den *Backoff-Stages* h bis m erreicht. Die Wahrscheinlichkeit, einen Backoff-Zähler in diesem Bereich zu ziehen, ist in Gleichung 5.41 angegeben.

$$Pr(r) = \sum_{k=h}^{m} \frac{d(k)}{CW_{max}+1} \quad \text{für } 2^{h-1}CW_{min}+1 \leq r \leq CW_{max} \tag{5.41}$$

5.5.6 Berechnung des Sättigungs-Durchsatzes der EDCF

Für die Leistungsbewertung eines Kommunikationsnetzes wird häufig die maximale Datenrate untersucht. Im Kontext der DCF bei IEEE 802.11 wird dabei häufig von Sättigungsdurchsatz gesprochen (vgl. [5]). Dabei ist der Sättigungsdurchsatz als Quotient von Payloadgröße durch die Übertragungszeit definiert. Um die Übertragungszeit, also die Gesamtdauer inklusive eventueller Kollisionen, für die Payload zu berechnen, werden die oben beschriebenen Markov-Modelle verwendet. Bei der DCF kann in einem *timeslot* grundsätzlich entweder übertragen oder nicht übertragen werden. Dabei kann bei einer Übertragung noch zwischen einer erfolgreichen Übertragung und einer Kollision unterschieden werden. Nachfolgend werden die Eintrittswahrscheinlichkeiten dieser Ereignisse bestimmt. Die Wahrscheinlichkeit einer erfolgreichen Übertragung wird mit P_{succ} gekennzeichnet, die einer Kollision mit P_{col}. Die Wahrscheinlichkeit, dass keine Übertragung in einem *timeslot* durchgeführt wird, wird mit P_{idle} bezeichnet.

Eine erfolgreiche Übertragung findet nur dann statt, wenn gleichzeitig kein anderer Nutzer auf das Netz zugreift, weder Nutzer der eigenen noch solche der anderen Zugriffskategorie.

$$\begin{cases} P_{succA} = n_A \cdot \tau_A \cdot (1-\tau_A)^{n_A-1} \cdot (1-\tau_B)^{n_B} \\ P_{succB} = n_B \cdot \tau_B \cdot (1-\tau_B)^{n_B-1} \cdot (1-\tau_A)^{n_A} \end{cases} \tag{5.42}$$

Bei einer Kollision greifen mehr als ein Nutzer gleichzeitig auf den Kanal zu. Dies geschieht genau dann, wenn nicht alle Nutzer nicht übertragen und weder ein Nutzer der Zugriffskategorie A noch der Kategorie B erfolgreich auf den Kanal zugreift. Mathematisch wird P_{col} wie folgt ausgedrückt:

$$P_{col} = 1 - P_{idle} - P_{succA} - P_{succB} \tag{5.43}$$

Dabei wird die Wahrscheinlichkeit, dass alle Nutzer nicht übertragen, als P_{idle} bezeichnet.

$$P_{idle} = (1-\tau_A)^{nA} \cdot (1-\tau_B)^{nB} \tag{5.44}$$

Der Erwartungswert der so genannten effektiven Payloadgröße $E[A]$ ist das Produkt aus der tatsächlichen Größe des Payload $E[P]$ mit der Wahrscheinlichkeit einer erfolgreichen Übertragung P_{succ}.

$$E[A] = P_{succA} \cdot E[P] \qquad E[B] = P_{succB} \cdot E[P] \tag{5.45}$$

Der Erwartungswert für die Dauer von zwei aufeinander folgenden Übertragungen wird mit EZ bezeichnet.

$$EZ = (P_{succA} + P_{succB}) \cdot T_s + P_{col} \cdot T_c + P_{idle} \cdot timeslot \tag{5.46}$$

Dabei steht T_s für die Dauer einer erfolgreichen Übertragung und T_c für die Dauer einer Kollision. Die Zusammensetzung dieser beiden Zeitspannen wird in den Abbildungen 5.12 und 5.13 dargestellt.

Abbildung 5.12: Dauer T_s einer erfolgreichen Payload-Übertragung

Abbildung 5.13: Dauer T_c einer Kollision bei einer Payload-Übertragung

Wie weiter oben beschrieben ergibt sich daraus der gesuchte Sättigungsdurchsatz S_A bzw. S_B für jeden Nutzer der Zugriffskategorie $\mathrm{AC_A}$ bzw. $\mathrm{AC_B}$. In Gleichung 5.47 repräsentiert n_a die Anzahl der $\mathrm{AC_A}$ und n_b die Anzahl der $\mathrm{AC_B}$ Stationen.

$$S_A = \frac{E[A] \cdot n_a}{EZ} \qquad S_B = \frac{E[B] \cdot n_b}{EZ} \tag{5.47}$$

5.6 Leistungsbewertung der EDCF

Um die Leistung der im Rahmen dieser Arbeit vorgestellten EDCF bewerten zu können, werden vier verschiedene Untersuchungen durchgeführt. Zunächst wird am Beispiel der Zugriffskategorie 1 eine detaillierte Analyse anhand von zwei Szenarien durchgeführt. Dabei kommt sowohl das oben vorgestellte analytische Modell zum Einsatz als auch eine Simulation, die später beschrieben wird. Die zweite Untersuchung analysiert die Leistungsfähigkeit aller Zugriffskategorien im direkten Wettbewerb von zwei Nutzern, die jeweils eine der neuartigen Zugriffskategorien verwenden. Daraus ergibt sich ein Vergleich des Durchsatzes aller Zugriffskategorien. Auch hier kommen analytisches Modell und Simulation zum Einsatz. Anschließend wird die Leistungsfähigkeit der neuen EDCF mit der EDCA aus dem IEEE 802.11e auf Basis des analytischen Modells verglichen. Zuletzt wird noch eine experimentelle Untersuchung durchgeführt, welche die zuvor erzielten Ergebnisse validieren soll.

5.6.1 Detaillierte Analyse der Zugriffskategorie 1

Für die detaillierte Analyse der Zugriffskategorie 1 (AC_1) werden zwei beispielhafte Szenarien betrachtet. Das erste Szenario untersucht den Wettbewerb von einem EDCF-Nutzer, der mit der Zugriffskategorie AC_1 priorisiert ist, mit gewöhnlichen, nicht bevorzugten WLAN-Nutzern. Daher wird der Durchsatz eines einzelnen EDCF-Nutzers untersucht, welcher beispielsweise die Parameter der AC_1 verwendet, in einer Gruppe von gewöhnlichen WLAN DCF-Nutzern ohne Priorisierung.

Das zweite Szenario untersucht die QoS-Priorisierung unterschiedlicher Gruppen. Hierbei wetteifert eine Gruppe von Nutzern der AC1 mit einer Gruppe von Nutzer

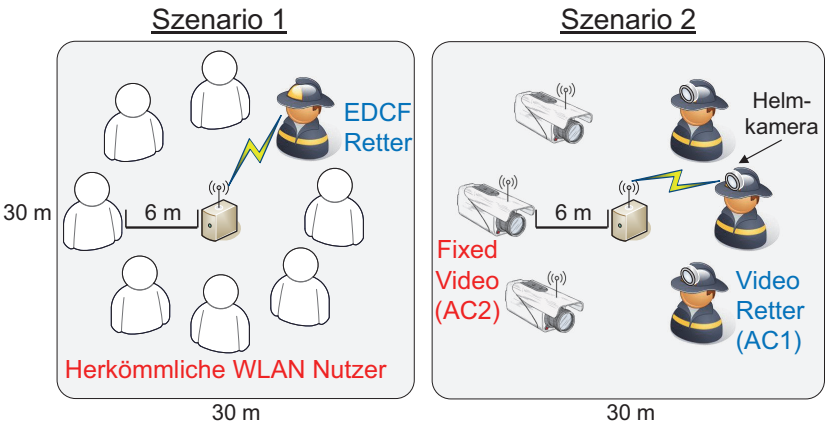


Abbildung 5.14: Links: Ein priorisierter gegen viele gewöhnliche, nicht bevorzugte WLAN-Nutzer. Rechts: Retter mit Video-Priorisierung gegen statische Kameras.

der AC2 (statische Videokameras) um den Kanalzugriff. Die Leistung der vorgestellten Emergency-DCF wird mittels der Analyse des Sättigungsdurchsatzes untersucht. Es wird erwartet, dass Nutzer, die eine höhere Priorität haben, einen höheren Durchsatz erzielen.

Die beiden soeben beschriebenen Szenarien sind in Abbildung 5.14 dargestellt. Auf der linken Seite der Abbildung wird das Bewertungsszenario für die Priorisierung der AC_1 über herkömmliche WLAN-Nutzer gezeigt. Dabei wetteifert ein einzelner Nutzer, der die EDCF nutzt, mit mehreren Nutzern, welche die herkömmliche WLAN DCF nutzen. In einem ersten Schritt wird der Durchsatz analysiert, wenn ein EDCF-Nutzer gegen einen herkömmlichen DCF-Nutzer antritt. In den folgenden Schritten wird die Anzahl der Nutzer mit dem herkömmlichen WLAN bis auf 30 erhöht, wobei immer nur ein einzelner EDCF-Nutzer gegen eine Gruppe von herkömmlichen WLAN-Nutzern antritt. Das Szenario ist so dimensioniert, dass sich alle Knoten miteinander in Kommunikationsreichweite befinden. Die Kommunikation findet zwischen einem Access Point im Zentrum des Szenarios und den WLAN-Nutzern, bzw. dem EDCF-Retter, die sich im Abstand von 6 Metern zum Access Point befinden, statt. In dem 30 m·30 m großen Szenario befinden sich keine Hindernisse und keine Wände. Die Nutzer bewegen sich nicht.

Das zweite Szenario ist auf der rechten Seite von Abbildung 5.14 zu sehen. In diesem Szenario wird der Sättigungsdurchsatz von AC1 (Helmkameras) und AC2 (stationäre Kameras) verglichen, wobei beide Nutzergruppen um den Kanalzugriff konkurrieren. Für jeden Vergleich sind die Anzahl der Nutzer pro Nutzergruppe

immer gleich. Zunächst werden die Sättigungsdurchsätze von jeweils einem AC1- und einem AC2-Nutzer, die auf den gleichen Kanal zugreifen wollen, untersucht. Die Abmessungen sind mit Szenario 1 identisch. Auch in Szenario 2 wird keine Mobilität betrachtet.

Die anhand des analytischen Modells berechneten Ergebnisse wurden zusätzlich mittels einer Simulationsumgebung validiert. Dazu wurde der Netz-Simulator OMNeT++ in der Version 4.1 [32] in Kombination mit dem INET Framework verwendet. Ferner wurde das existierende IEEE 802.11b Modell des INET Frameworks um die Emergency-DCF erweitert. Die Ergebnisse der beiden Szenarien wurden in [101] veröffentlicht.

In Abbildung 5.15 ist ein Screenshot des Szenarios in der OMNeT-Simulationsumgebung dargestellt. In dem beispielhaften Szenario wetteifern sechs AC1-Knoten mit sechs AC2-Knoten um den Kanal. Die Abstände der Knoten im Szenario sind so gewählt, dass alle Knoten miteinander kommunizieren können. Der Durchsatz wird zwischen den Knoten und dem AP gemessen. Der AP ist dabei die Kommunikationssenke. Die Knoten sind alle im gleichen Abstand vom AP positioniert.

Die Simulationsparameter sind in Tabelle 5.3 aufgeführt. Es wird ein statisches 802.11b WLAN bei 2,4 GHz simuliert, bei dem ein Freiraummodell zum Einsatz kommt.

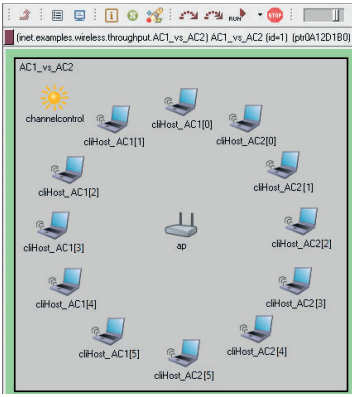


Abbildung 5.15: OMNeT-Szenario

Tabelle 5.3: Simulationsparameter

Parameter	Wert
WLAN Standard	802.11b
Frequenz	2,4 GHz
Bitrate	11 Mbps
Sendeleistung	20 mW
Rauschschwelle	−110 dBm
Empfindlichkeit	−85 dBm
Mobilität	keine
Ausbreitungsmodell	Freiraum
Pfadverlustkoeffizient γ	2

Ergebnisse

Die in den Ergebnisgraphen dargestellten Linien stehen für Folgendes: Die blaue Linie bzw. der blau ausgefüllte Kreis beschreibt den analytisch ermittelten Durchsatz eines Nutzers der Kategorie AC_A aus einer Menge von n Nutzern (n ist variabel auf der x-Achse), die rote Linie bzw. das ausgefüllte rote Dreieck zeigt den analytisch

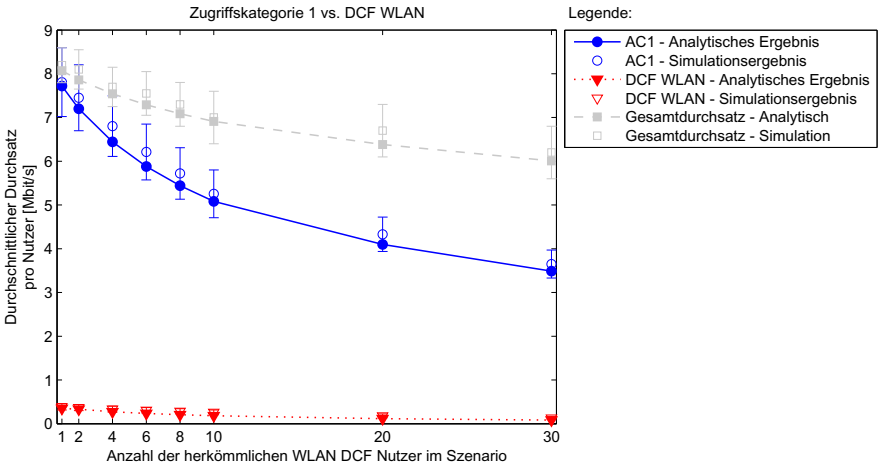


Abbildung 5.16: Durchschnittlicher Durchsatz von einem AC1 Nutzer in Abhängigkeit einer steigenden Gruppengröße von DCF Nutzern

ermittelten Durchsatz eines AC_B-Nutzers aus einer Menge von n Nutzern, und die graue Linie bzw. das grau ausgefüllte Quadrat zeigt den Gesamtdurchsatz des Szenarios in Abhängigkeit von der Nutzeranzahl n pro Zugriffskategorie. Die Simulationsergebnisse sind mittels nichtausgefüllter Symbole einschließlich der Standardabweichung in die Grafik eingetragen. Da Zugriffskategorie-Kombinationen untersucht wurden, bei der die AC_A höher priorisiert ist als die AC_B, haben Nutzer der Kategorie AC_A immer einen höheren Durchsatz als Nutzer der Kategorie AC_B.

Durchsatzanalyse von Szenario 1 (AC 1 vs. DCF)

Abbildung 5.16 zeigt den durchschnittlich erreichten Durchsatz im ersten Szenario für einen Nutzer, der mit der AC1 priorisiert ist, im Wettbewerb mit einem oder mehreren herkömmlichen WLAN Nutzern ohne Priorisierung. Der erreichte Durchsatz des priorisierten EDCF-Nutzers ist immer höher als der Durchsatz der herkömmlichen IEEE 802.11-Nutzer, was die Priorisierung bestätigt. Herkömmliche IEEE 802.11-Nutzer haben keine Möglichkeit auf einen Kanalzugriff, was vergleichbar mit der Situation beim DCF-Fehlverhalten ist (siehe dazu [87] und [60]). Aufgrund der Kollisionen, welche durch den gleichzeitigen Kanalzugriff verursacht werden, sinkt der Gesamtdurchsatz mit steigender Anzahl der Nutzer im System.

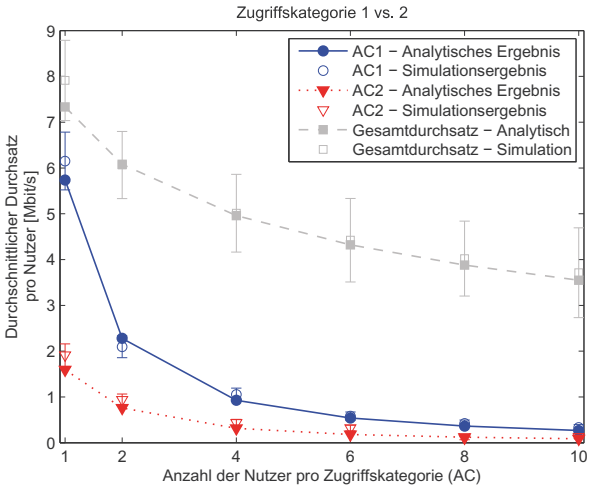


Abbildung 5.17: Durchschnittlicher Durchsatz von AC1 und AC2 Nutzern bei steigender Gruppengröße

Selbst bei 30 herkömmlichen DCF Nutzern, die um den Kanalzugriff wetteifern, erreicht der mit der Zugriffskategorie AC1 priorisierte Nutzer noch einen durchschnittlichen Durchsatz von ca. 3,5 Mbit/s. Die herkömmlichen WLAN-Nutzer erhalten in dieser Situation nur wenige kbit/s.

Durchsatzanalyse von Szenario 2 (AC 1 vs. AC 2)

Abbildung 5.17 zeigt das Ergebnis der Leistungsbewertung des zweiten Szenarios. Es zeigt den durchschnittlichen Durchsatz von jeweils einem AC1-Nutzer und einem AC2-Nutzer in Abhängigkeit von einer steigenden Anzahl an Nutzern pro Zugriffskategorie. Alle Nutzer befinden sich im Wettbewerb um den Kanal.

Im Wettbewerb eines AC1-Nutzers mit einem AC2-Nutzer erreicht der AC1 Nutzer mit ca. 5,8 Mbit/s einen deutlich höheren Durchsatz im Vergleich zum AC2-Nutzer, der nur 1,8 Mbit/s im Durchschnitt erhält. Mit steigender Gruppengröße wird der Unterschied jedoch immer geringer und sinkt auf wenige hundert kbit/s pro Nutzer beim Wettbewerb von 10 AC1- gegen 10 AC2-Nutzern ab.

Die steigende Gruppengröße führt zu häufigen Kollisionen, was zu einem deutlich reduzierten Gesamtdurchsatz bei großen Gruppen führt. So beträgt der durchschnittliche Gesamtdurchsatz im Szenario „ein AC1-Nutzer vs. einen AC2-Nutzer“ ca. 7,5 Mbit/s. Der Gesamtdurchsatz sinkt im Szenario „10 AC1-Nutzer vs. 10

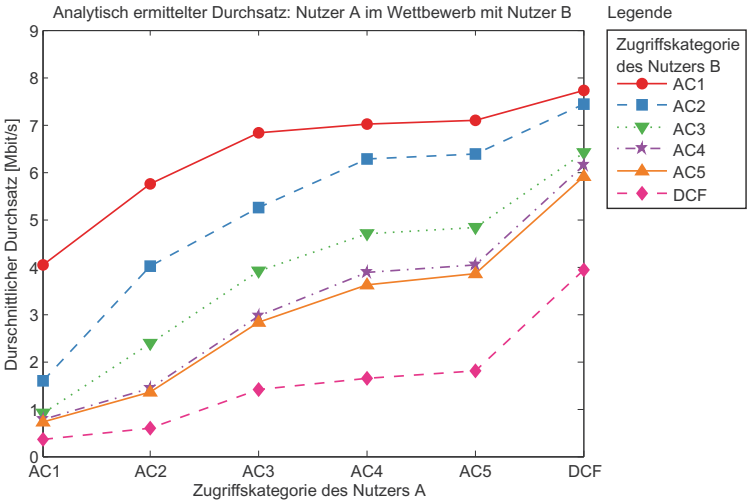


Abbildung 5.19: Analytisch ermittelter Durchsatz von Nutzer A

AC2-Nutzer“ auf ca. 3,7 Mbit/s ab, was ca. einer Halbierung des Gesamtdurchsatzes im „1 vs. 1“-Fall entspricht.

5.6.2 Vergleich des Durchsatzes der Zugriffskategorien

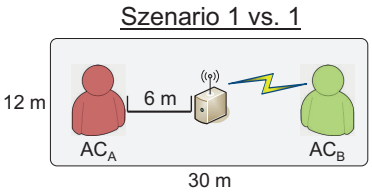


Abbildung 5.18: Szenario 1vs.1

Zusätzlich zu den zuvor beschriebenen Szenarien wurde die Effektivität der Priorisierung der einzelnen Zugriffskategorien verglichen. Dazu wurde der Durchsatz, den ein Nutzer einer bestimmten Zugriffskategorie A (AC_A) im Wettbewerb mit einem Nutzer der Zugriffskategorie B (AC_B) erzielt, sowohl analytisch als auch simulativ ermittelt. Dieses *1 vs. 1* genannte Szenario ist in Abbildung 5.18 dargestellt.

In Abbildung 5.19 ist der analytisch ermittelte Durchsatz eines Nutzers der einzelnen Zugriffskategorien im Wettbewerb mit einem Nutzer einer anderen Zugriffskategorie aufgetragen. Wie erwartet, erzielt der Nutzer der AC1 im Wettbewerb mit allen anderen Kategorien den höchsten Durchsatz. Ein nicht priorisierter Nutzer, der also die herkömmliche WLAN DCF verwendet, erzielt im Wettbewerb immer den niedrigeren Durchsatz.

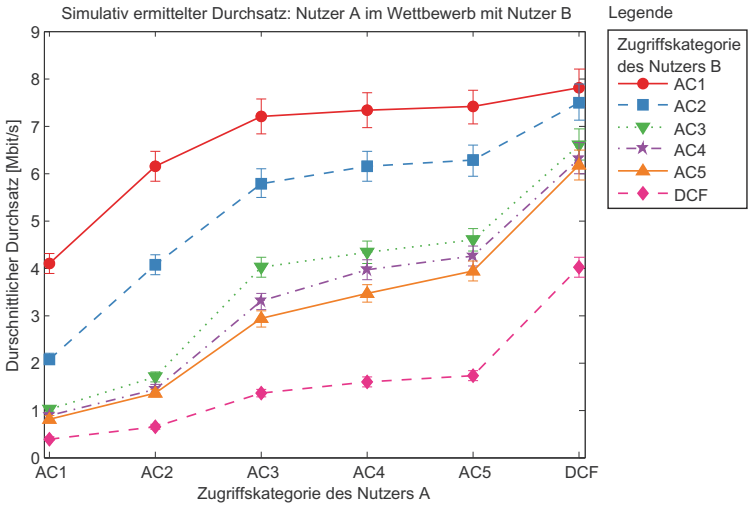


Abbildung 5.20: Simulativ ermittelter Durchsatz von Nutzer A

Der Verlauf der Kurven für den Durchsatz der AC4 und AC5 sind sehr ähnlich. Dies ist auf die ähnliche Parametrisierung zurückzuführen, wobei die AC4 jedoch stets eine höhere Datenrate erzielt als die AC5.

In Abbildung 5.20 ist das Ergebnis der Simulation des zuvor mit dem analytischen Modell untersuchten Durchsatzes dargestellt. Der Verlauf der Kurven deckt sich im Wesentlichen mit den Ergebnissen aus dem analytischen Modell. Die Ergebnisse der Simulation sind mit leichten Schwankungen behaftet, wie die Standardabweichung zeigt.

Zusammenfassend lässt sich feststellen, dass die gewünschte Priorisierung für den Katastrophenschutz mittels der vorgeschlagenen EDCF den gewünschten Leistungsgewinn erzielt.

5.6.3 Vergleich der neuen EDCF Zugriffskategorien mit 802.11e

Nachdem gezeigt wurde, dass die Priorisierung der neuen Zugriffskategorien untereinander und gegenüber der herkömmlichen WLAN DCF funktioniert, soll nun untersucht werden, ob auch eine Priorisierung gegenüber den Zugriffskategorien der IEEE 802.11e (EDCA) erreicht werden kann. Analog zum vorherigen Abschnitt wird dazu der erreichte Durchsatz von einem Nutzer, der mittels der EDCF priorisiert wird, in Konkurrenz zu einem Nutzer, der mittels der EDCA der IEEE 802.11e

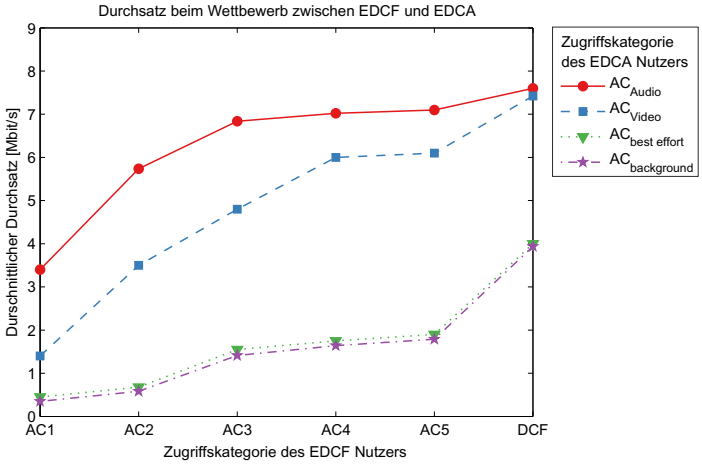


Abbildung 5.21: Durchsatz im Wettbewerb von EDCF mit EDCA

priorisiert wird, untersucht. Es werden alle Kombinationen der Zugriffskategorien der EDCF und der EDCA geprüft.

In Abbildung 5.21 ist das Ergebnis der Untersuchung dargestellt. Der Verlauf der Kurven zeigt, dass die höchste Priorisierung der EDCF immer eine höhere Datenrate erzielt als alle Priorisierungsklassen der IEEE 802.11e. Insbesondere bedeutet dies, dass Die AC_1 eine höhere Priorisierung als die AC_{Audio} ermöglicht.

Auch im Vergleich mit IEEE 802.11e lässt sich zusammenfassend feststellen, dass die gewünschte Priorisierung für den Katastrophenschutz als Anwender mittels der vorgeschlagenen EDCF den gewünschten Leistungsgewinn erzielt.

5.6.4 Experimentelle Untersuchung

Nachdem die simulativen und analytischen Ergebnisse gezeigt haben, dass die Priorisierung der Rettungskräfte mittels der neuen EDCF möglich ist, soll nun in einem Experiment überprüft werden, ob eine Priorisierung mittels EDCF auch in der Praxis im gleichen Maße besteht. Der Aufbau des Experiments ist in Abbildung 5.22 dargestellt. Der Abstand von 20 cm wurde gewählt, um den Einfluss der Dämpfung aufgrund der Entfernung möglichst klein zu halten. Das Experiment besteht aus vier *Dropped Units*, wobei zwei *Dropped Units* das Feuerwehr-Netz repräsentieren, welches durch die EDCF priorisiert wird und zwei *Dropped Units* ein lokales Netz am Einsatzort repräsentieren, welches das Feuerwehr-Netz stört. Für die Validierung des Priorisierungskonzepts in der Praxis wurde der WLAN-Treiber

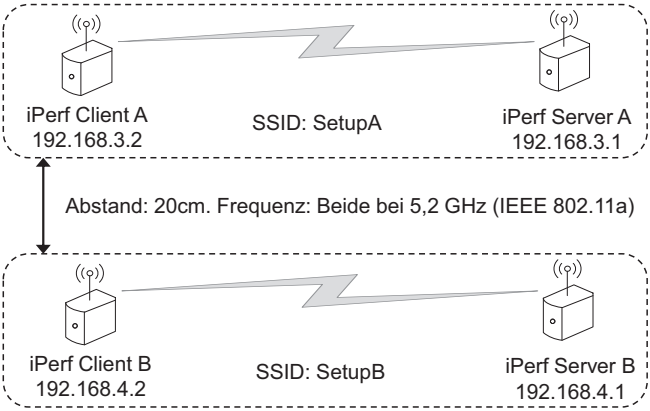


Abbildung 5.22: Messaufbau zur Validierung der EDCF

der *Dropped Units* (siehe Kapitel 3.2) so modifiziert, dass die CW-Parameter der EDCF angepasst werden können. Dazu sind im Treiber die Werte von den Standard IEEE 802.11e-Parametern auf die Werte der EDCF geändert worden, wobei alle AIFSN auf den Wert 2 eingestellt wurden. Der Parameter SIFS wurde nicht angepasst. Bei dieser Konfiguration basiert die Priorisierung also nur auf den unterschiedlich großen Wettbewerbsfenstern.

Für die Experimente wurden Embedded PCs vom Typ Overo der Firma Gumstix verwendet, die mit einem Linux Betriebssystem arbeiten. Es wird ein Kernel mit der Version 3.4.0-rc6 eingesetzt. Für den Betrieb des WLAN-USB-Sticks vom Typ DWA-160 der Firma D-Link wird der Treiber carl9170 verwendet. Es ist dabei wichtig, die Treiber-Option $noht = 1$ zu setzen, damit die Untersuchung von QoS-Parametern durchgeführt werden kann. Mittels der Option $noht = 1$ wird die *frame aggregation* abgeschaltet. Dieses Feature wird in 802.11e genutzt, um höhere Datenraten zu erzielen, indem mehrere Daten-Frames gebündelt versendet werden. Dabei wird der Header eingespart, der immer mit niedrigen Datenraten (<2 Mbit/s) versendet wird, auch wenn der Kanal höhere Datenraten erlaubt. Der im Experiment verwendete Treiber unterstützt jedoch dieses Feature nicht, wenn QoS-Kategorien verwendet werden sollen. Die *frame aggregation* ist daher abzuschalten.

Der Versuchsaufbau ist in Abbildung 5.22 dargestellt. Für die Messung wird folgende Konfiguration des WLAN-Netzes verwendet: Das Experiment wird im Adhoc-Modus bei 5,2 GHz durchgeführt. Insgesamt besteht die Konstruktion aus vier Knoten, wobei sich jeweils zwei Knoten in einem IBSS befinden, und alle vier Knoten auf dem gleichen Kanal kommunizieren.

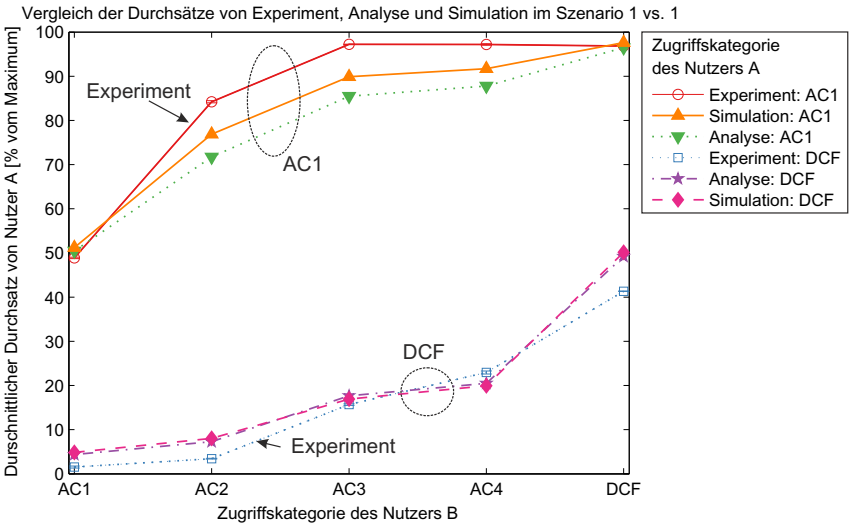


Abbildung 5.23: Relative Durchsätze von Messung, Analyse und Simulation

Für die Messung wird das Programm iPerf in Version 2.0.5-2.1 (Debian) verwendet. iPerf kann für eine Messung explizit eine bestimmte QoS-Kategorie verwenden. Im Nachfolgenden wird zunächst der Aufruf von iPerf mit QoS- und anschließend ohne QoS-Unterstützung gezeigt:

```
iperf -S 0xE0 -c 192.168.3.1 -u -b 20M -i 1 -t 60 (mit QoS)
iperf -c 192.168.4.1 -u -b 20M -i 1 -t 60 (ohne QoS)
```

Beide Aufrufe sind sehr ähnlich. Der Parameter `-S 0xE0` gibt iPerf an, dass die QoS-Kategorie E0 genutzt werden soll. In dem Treiber der WLAN-Hardware wird E0 der EDCF-Kategorie AC1 zugeordnet. An dem Befehl ist außerdem zu erkennen, dass der Client bei iPerf die QoS-Kategorie auswählt.

Für die experimentelle Leistungsbewertung wurden 25 Messungen durchgeführt. Jede Zugriffskategorie (AC) wird gegen alle anderen getestet. Dabei bleibt die untersuchte AC im Netz 1 aktiv, während im Netz 2 jeweils alle anderen Kategorien wiederholt aufgerufen werden.

In Abbildung 5.23 wird das Messergebnis zusammen mit den Ergebnissen aus dem analytischen Modell und der Simulation gezeigt. Dargestellt werden die Zugriffskategorie 1 (AC_1) und die DCF. Aufgrund der unterschiedlichen maximalen

Datenraten von 802.11a und 802.11b wurden die Ergebnisse auf den jeweiligen maximal erreichten Wert skaliert.

Die Kurvenverläufe von Experiment, Simulation und analytischem Modell sind größtenteils ähnlich, wobei beim Experiment die maximale Datenrate schneller erreicht wird als bei den anderen Untersuchungsverfahren. Wenn der Nutzer A mit der AC1 priorisiert ist, so erreicht er in dem untersuchten Szenario mindesten 50% der Datenrate. Er „gewinnt“ also den Wettbewerb gegen alle anderen Zugriffskategorien und gegen die DCF.

Die DCF „verliert“ den Wettbewerb gegen alle anderen Zugriffskategorien. Dies ist insbesondere bei den Wettbewerben gegen AC1 und AC2 zu sehen. Es wird weniger als 10% der maximalen Datenrate erreicht. Im Wettbewerb mit AC3 und AC4 bleibt die DCF unterhalb der Datenrate, die im Wettbewerb DCF gegen DCF erreicht wird. Beim Wettbewerb DCF gegen DCF wird, ähnlich wie beim Wettbewerb AC1 gegen AC1, ca. 50% der maximalen Datenrate von beiden DCF-Clients erreicht.

Dieses Ergebnis zeigt, dass die Priorisierung mittels der Zugriffskategorien der EDCF auch in der prototypischen Umsetzung funktioniert. Dabei reicht in dem betrachteten Szenario die Priorisierung mittels unterschiedlich großer Wettbewerbsfenster aus. Die Anpassung der SIFS Dauern ist für die Priorisierung hier nicht zwingend erforderlich.

5.7 Zusammenfassung

In diesem Kapitel wurde ein neuer Parametersatz für die DCF vorgestellt, welcher Dienstgüte in Szenarien des Katastrophenschutzes ermöglicht. Dieser Parametersatz wird Emergency-DCF (EDCF) genannt. Es werden fünf neue Zugriffskategorien definiert, welche für die unterschiedlichen Kommunikationskategorien im Katastrophenschutz stehen. Dabei werden alle neuen Kommunikationskategorien gegenüber der herkömmlichen DCF-basierten IEEE 802.11-Kommunikation priorisiert übertragen. Für die Leistungsbewertung der EDCF wurde ein existierendes Markov-Modell angepasst und erweitert. Anhand dieses erweiterten Modells wurde dann der Sättigungsdurchsatz analysiert. Die analytisch ermittelten Ergebnisse wurden mittels einer Simulation verifiziert. Es wurden zwei Szenarien analysiert: Im ersten Szenario wurde überprüft, ob EDCF-Nutzer immer einen höheren Sättigungsdurchsatz erzielen als ursprüngliche IEEE 802.11-Nutzer. Das zweite Szenario untersucht die Dienstgüte-Unterstützung der EDCF. Dabei wird der Sättigungsdurchsatz von zwei unterschiedlichen Zugriffskategorien untersucht. Die Ergebnisse der Leistungsbewertung zeigen, dass der hier vorgeschlagene Parametersatz für die eine zuverlässige Kommunikation in untersuchten Szenarien ermöglicht. Dies gilt selbst dann, wenn ursprüngliche WLAN-Netze am Einsatzort existieren.

6

Leistungsbewertung des prozesskonformen Netzaufbaus

In diesem Kapitel wird die Leistungsfähigkeit in Bezug auf das Packet Delivery Ratio, kurz PDR, und die Paket-Verzögerung des in Kapitel 4 beschriebenen Schlauchkonzepts evaluiert. Wird das neuartige Schlauchkonzept eingesetzt, bauen Rettungskräfte das Ad-hoc-Netz on-the-fly auf, wenn sie Feuerwehrschläuche verlegen. Nachfolgend werden das PDR und die Paket-Verzögerung des neuen Konzepts mit existierenden Methoden verglichen, bei denen die WLAN-Router an vorher berechnete Positionen gelegt werden. Um diese Positionen zu berechnen, wird ein auf Steinerbäumen basierender Optimierungsansatz angewendet. Es werden drei unterschiedlich große Szenarien untersucht, wobei sowohl die Anzahl der WLAN-Router als auch die Anzahl der Sender steigt. Anhand der Ergebnisse wird gezeigt, dass die Leistungsfähigkeit des neuen Schlauchkupplungsansatzes vergleichbar ist zu den Ergebnissen bei optimierten Positionen. Hierbei ist die Verwendung des Schlauchkonzepts jedoch komfortabler für den Feuerwehrmann, sowohl beim Aufbau des Netzes, als auch beim Einsammeln der InCo Units nach Einsatzende. Abschließend wird die Erprobung des prozesskonformen Netzaufbaus als Feldtest bei der Feuerwehr Gelsenkirchen beschrieben. Es wird gezeigt, dass ein Video von einer Helmkamera über mehrere InCo Units zum Einsatzleitwagen übertragen werden kann.
Die in den Abschnitten 6.1 bis 6.3 dieses Kapitels beschriebenen Konzepte und Ergebnisse bauen auf Beiträgen des Autors zur Publikation [99] auf.

6.1 Einleitung

Im Rahmen dieser Arbeit wird als Szenario ein Brand in einer Ausstellungshalle der Messe Köln angenommen. In Abbildung 6.1 ist ein 3D Modell der Messe in Köln dargestellt. Die Flamme symbolisiert den angenommenen Brand in Halle 8.

Im Gespräch mit dem Betreiber der Messe und der Feuerwehr wurde erörtert, wie ein solcher Brand bekämpft werden würde. Da sich die betroffene Halle am nördlichen Rand der Messe befindet, kommen die Rettungskräfte auf einer Zufahrt zum

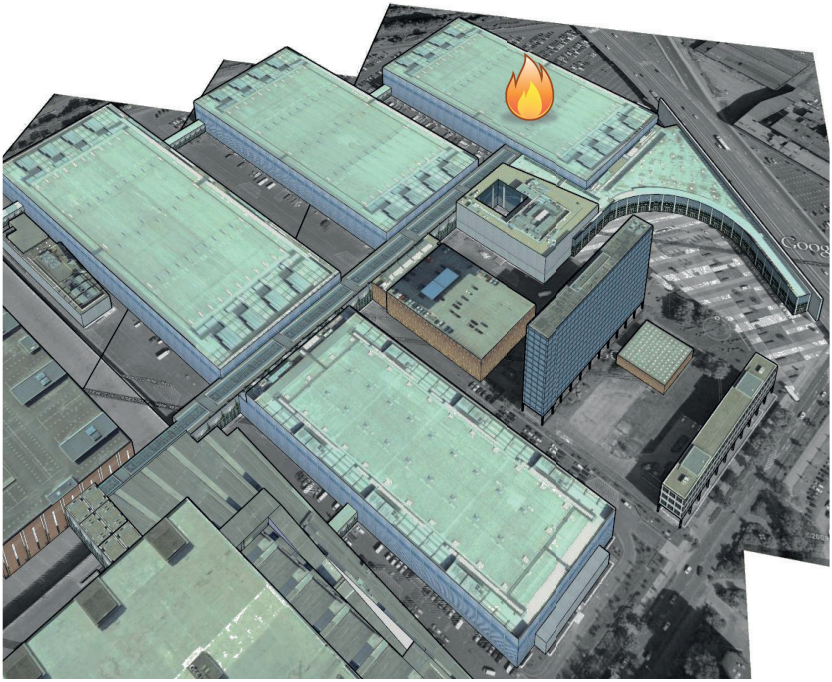


Abbildung 6.1: 3D Modell der Messe in Köln

„Tor-Nordeingang“ auf das Messegelände. Bei unklarer Lage schickt der Disponent der Feuerwehr nach Eingang des Brand-Alarms zunächst einen Löschzug zum Schadensort. Ein Löschzug besteht bei der Feuerwehr aus einem Führungsfahrzeug (Einsatzleitwagen - ELW), einem Löschgruppenfahrzeug, einem Tanklöschfahrzeug und einem Hubrettungsfahrzeug (Drehleiter). Das Führungsfahrzeug wird in sicherem Abstand zum Schadensort abgestellt. Von dort aus ist der Einsatzleiter aktiv und steuert die übrigen Rettungskräfte.

In diesem Szenario stellt der Einsatzleiter die Senke des Datenverkehrs dar. Es wird angenommen, dass die Besatzung des Löschgruppenfahrzeugs mit Helmkameras ausgestattet ist. Während des Einsatzes senden die Helmkameras jeweils ein Video mit konstanter Bitrate an den Einsatzleiter.

Es wird ferner angenommen, dass das Führungsfahrzeug in der Nähe eines Hydranten parkt, an den das Tanklöschfahrzeug angeschlossen wird. Das Löschgruppenfahrzeug und das Hubrettungsfahrzeug parken näher am betroffenen Gebäude und sind per Feuerwehrschlauch mit dem Tanklöschfahrzeug verbunden. Ausgehend von diesen beiden, sich nah am Einsatzort befindlichen, Fahrzeugen rücken

die Feuerwehrleute zum Brand vor. Dabei legen sie einen Feuerwehrschlauch aus, um Löschwasser zum Brand zu transportieren.

Für die Leistungsbewertung des in dieser Arbeit vorgestellten prozesskonformen Netzaufbaus werden die beiden weit verbreiteten Routing-Protokolle *Optimized Link State Routing* (OLSR) [12] and *Better Approach To Mobile Ad-hoc Networking* (BATMAN) miteinander verglichen, welche aufgrund ihres proaktiven Verhaltens für den Einsatz in Großschadenslagen geeignet sind. Die beiden Protokolle und werden in Kapitel 2.1.3 vorgestellt. Eine Leistungsbewertung der beiden Protokolle findet sich bei *Barolli et al.* in [3].

Der hier vorgeschlagene Vernetzungsansatz wird anhand des SPIDER Anwendungsszenarios untersucht. Bei diesem Szenario handelt es sich um ein Feuer innerhalb einer Ausstellungshalle auf einem Messegelände. Aufgrund der Komplexität des Szenarios wird die Leistungsbewertung mit Hilfe einer Simulation durchgeführt. Um eine realitätsnahe Simulation durchführen zu können, wurde zunächst ein Experiment mittels eines realen Versuchsaufbaus durchgeführt und die gewonnen Parameter in die Simulation übernommen. Anschließend ist der Versuchsaufbau in der Simulationsumgebung nachgebildet worden, und die Ergebnisse der simulativen Leistungsbewertung sind mit den realen Messwerten validiert worden. Nach der Validierung ist die Simulationsumgebung angepasst worden, damit der hier vorgestellte prozesskonforme Netzaufbau für Großschadenslagen abgebildet werden kann.

Dieses Szenario wird im Folgenden für die Bewertung der Leistung des prozesskonformen Netzaufbaus herangezogen. Zunächst wird die resultierende Netztopologie beschrieben. Anschließend wird die Modellierung des Szenarios in der Simulationsumgebung beschrieben. Mit Hilfe der Simulationsumgebung kann die Leistungsbewertung durchgeführt werden, wobei die durchschnittliche Verzögerung der Übertragung zwischen den Feuerwehrleuten und dem Einsatzleiter und die Paket-Auslieferungsrate auf dieser Übertragungsstrecke ermittelt werden. Dieses Kapitel endet mit der Zusammenfassung der Ergebnisse der Leistungsbewertung. Teile der hier präsentierten Ergebnisse wurden in [99] veröffentlicht.

6.1.1 Resultierende Netztopologie

Wird das *InCo Unit* Konzept verwendet, also zwischen die Schlauchkupplungen der Feuerwehrschläuche eine *Dropped Unit* integriert, so führt dies zu einer Netztopologie, die in Abbildung 6.2 gezeigt ist. Ein Satellitenbild der Messehalle ist im Hintergrund der Abbildung 6.2 dargestellt. Das Szenario besteht aus einem blauen Knoten, der den Einsatzleiter (Empfänger) repräsentiert und die Daten von den Rettungskräften (Sender) empfängt, die in grün dargestellt sind. Sender und Empfänger sind mittels aktiver *InCo Units* miteinander verbunden, welche in Rot dargestellt sind. Inaktive *InCo Units* sind nicht dargestellt.

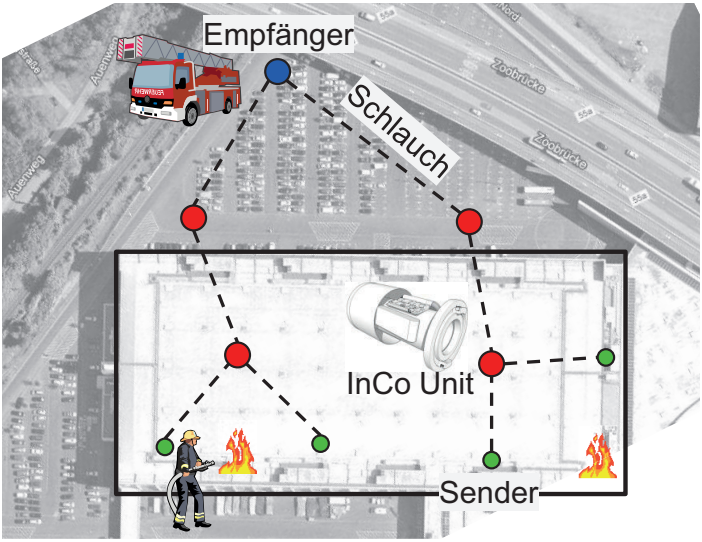


Abbildung 6.2: Kleines Anwendungsszenario einer Ausstellungshalle mit vier Sendern

Jede Rettungskraft hält eine Route zum Einsatzleiter aufrecht, was zu einer Multi-Hop-Verbindung zwischen Rettungskräften und Einsatzleiter über mehrere *InCo Units* führt. Aufgrund der relativ kurzen Schlauchlänge von 20 Metern werden die *InCo Units* relativ häufig platziert. Dabei werden oft mehr *InCo Units* platziert als eigentlich nötig. Redundante *InCo Units*, die bei der Kommunikation übersprungen werden können, werden mittels des in Kapitel 4 beschriebenen Interferenz-Vermeidungs-Algorithmus deaktiviert.

Ausgehend von diesem Szenario werden die drei Szenarien „klein“, „mittel“ und „groß“ für die Leistungsbewertung abgeleitet. Das kleine Szenario stimmt mit dem Szenario aus Abbildung 6.2 überein. Durch eine Spiegelung am Einsatzleiter wird das mittlere Szenario erzeugt. Es befinden sich in diesem Szenario also doppelt so viele Sender und aktive *InCo Units*, aber nur ein Einsatzleiter. Für das große Szenario werden zusätzliche *InCo Units* und Sender auf der Mittelachse hinzugefügt. Die drei Szenarien sind in Abbildung 6.3 dargestellt.

Zusätzlich werden drei weitere Szenarien untersucht, bei der die Positionen der *InCo Units* beliebig gewählt werden können. Diese Szenarien sollen die Anwendung der Algorithmen TSA und TIA aus Kapitel 4.1 ermöglichen und somit einen Vergleich zu den Ergebnissen bei der Anwendung der *InCo Units* und des IAA liefern. Bei der beliebigen Positionierung der *InCo Units* soll eine vergleichbare

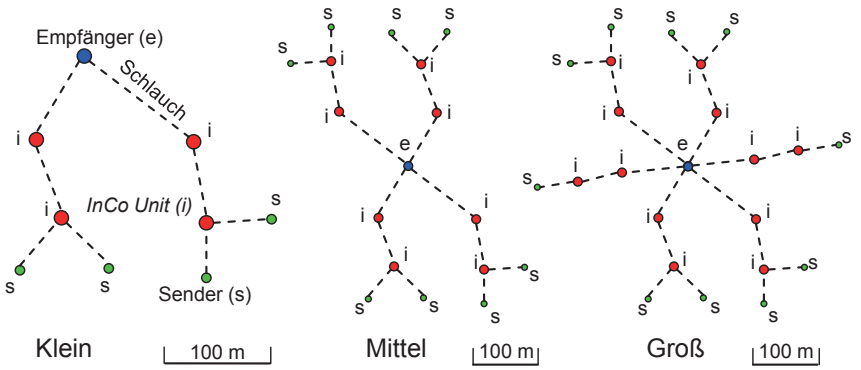


Abbildung 6.3: Drei Szenarien für die Leistungsbewertung

Abdeckung, wie sie bei der Anwendung des Schlauchkonzepts erreicht werden, mit dem Ziel, möglichst wenig *InCo Units* für die Abdeckung einzusetzen. Zusätzlich werden nah beieinander liegende Sender zusammengefasst. Die Datenrate der zusammengefassten Sender entspricht der Summe der Datenraten der einzelnen Sender. Diese zusätzlichen Szenarien dienen der Referenz. Da hier möglichst wenige *InCo Units* platziert werden sollen, wird die Platzierung der *InCo Units* in diesen Szenarien im Folgenden *minRouter-Strategie* genannt.

6.2 Simulationsbasierte Untersuchung

Um das Multi-Hop-Netz zu simulieren, werden die diskrete, ereignisbasierte Simulationsumgebung OMNeT++ [32] und das Framework INETMANET für OMNeT eingesetzt. Dabei bietet das INETMANET Modelle für die gängigen Netzwerkprotokolle und darüber hinaus auch die für das *InCo Unit*-Konzept interessanten Ad-hoc-Routing-Protokolle. Unter anderem zählen BATMAN und OLSR zu den unterstützten Protokollen. Typischerweise werden Routing-Protokolle in Ad-hoc-Szenarien für die Suche nach dem optimalen Pfad eingesetzt, wobei eine Metrik benutzt wird, die bei jedem Protokoll anders ist. In der Regel ist der optimale Pfad auch der kürzeste Pfad, was dazu führt, dass die Anzahl der Hops meist für die Pfadsuche zugrunde gelegt wird. In diesem Kontext sind die beiden in Kapitel 2.1.3 eingeführten, proaktiven Protokolle BATMAN und OLSR in der Praxis weit verbreitet, insbesondere in statischen Szenarien mit dynamischen Komponenten.

In Abbildung 6.2 ist das initiale Netzsetup dargestellt, welches für die Leistungsbewertung herangezogen wird. Alle WLAN-Router sind statisch, da der Einfluss der Routerpositionen auf die Leistung des Netzes untersucht werden soll. Für einen fairen Vergleich werden die Parameter der Protokolle für dieses Szenario im

Tabelle 6.1: Parameter der Simulationsumgebung
Grundlegendes Netz- und Verkehrsmodell

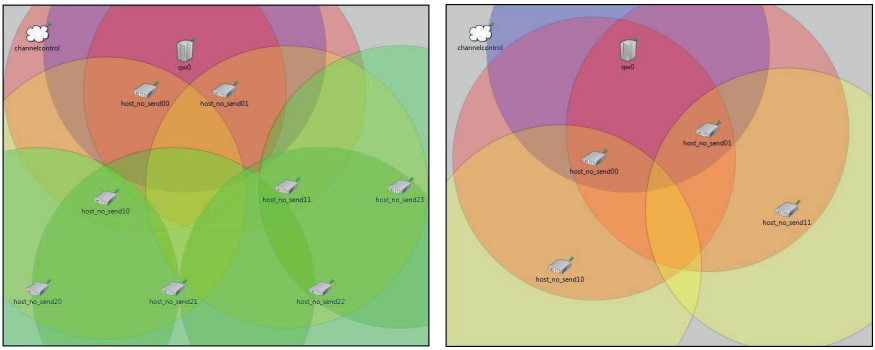
Parameter	Wert
Sendereichweite [m]	250
Mobilitätsmodell	Statisch
Antennentyp	Omni-direktional
Mac Layer	802.11a
Kanalmodell	Freiraum
Simulationsdauer [s]	300
Simulationswiederholungen	10
Verkehrsmodell	CBR-UDP
Paketgröße	1460 Bytes
Puffergröße [Pakete]	100

Szenarienspezifische Netz- und Verkehrsmodelle

Szenario	Knoten	Datenrate [kbit/s]	Sender
klein$_{IAAan}$	8	768	4
mittel$_{IAAan}$	16	768	8
groß$_{IAAan}$	22	768	10
klein$_{IAAaus}$	36	768	4
mittel$_{IAAaus}$	72	768	8
groß$_{IAAaus}$	92	768	10
klein$_{minRouter}$	4	1536	2
mittel$_{minRouter}$	8	1536	4
groß$_{minRouter}$	12	1536	6

Konfiguration der Protokoll-Parameter

Protokoll	Parameter | Wert	Beschreibung
BATMAN	OGM-Intervall | 1s	*Originator* Nachrichten sind für den Aufbau und die Aufrechterhaltung von Routen zwischen Knoten notwendig.
OLSR	HELLO-Intervall | 1s	*HELLO* Nachrichten werden für den Aufbau und die Aufrechterhaltung von Verbindungen zwischen direkten Nachbarknoten (ein-Hop) und zwei-Hop Knoten benötigt.
	TC-Intervall | 2s	*Topology Control* Nachrichten sind für den Aufbau und die Aufrechterhaltung von Routen zwischen Knoten notwendig.



Kleines Szenario: Inter Coupling (InCo) Strategie

Kleines Szenario: Min. Anzahl Relay Strategie

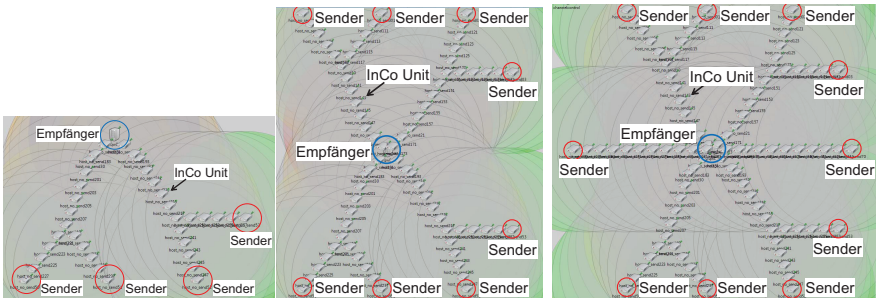
Abbildung 6.4: Modellierung des kleinen Szenarios in OMNeT

Hinblick auf die Paket-Auslieferungs-Rate (PDR) abgestimmt. Diese Parameter wurden durch Überprüfung unterschiedlicher Parameter ermittelt.

Die Antennen der *InCo Units* werden soweit herausgezogen, dass die Antennenhöhe keinen Einfluss mehr auf die Datenrate hat (siehe Kapitel 3.3). Um auch weitere Einflüsse auf den im Fokus stehenden Vergleich der Platzierungsmethoden zu vermeiden, wurde als Kanalmodell die Freiraumausbreitung gewählt. Eine Zusammenfassung der Konfiguration und des untersuchten Verkehrs ist in Tabelle 6.1 gegeben. Darüber hinaus werden die drei untersuchten Szenarien parametrisiert und die relevanten Protokollparameter angegeben. Die Modellierung des kleinen Szenarios mittels OMNeT++ ist in Abbildung 6.4 dargestellt. Auf der linken Seite der Abbildung ist die Vernetzung mittels der prozesskonformen Platzierung dargestellt. Rechts ist die Vernetzung mittels der *minRouter*-Strategie zu sehen.

Es werden drei verschieden große Szenarien analysiert, wobei die Anzahl der Router und die Anzahl der Sender vom kleinen über das mittlere bis zum großen Szenario ansteigen. In allen Szenarien ist ein einzelner Empfänger präsent, welcher den Einsatzleiter bei einer Großschadenslage darstellt. Die Positionen der Router in den einzelnen Szenarien sind entweder durch Optimierung unter Berücksichtigung einer möglichst geringen Anzahl von Routern ausgewählt worden, was mit *minRouter* gekennzeichnet wird, oder die Positionen haben sich aufgrund der prozessintegrieren Ausbringungsstrategie entlang von Feuerwehrschläuchen ergeben, was mit IAA gekennzeichnet wird.

Es werden zwei Varianten der prozessintegrieren Ausbringungsstrategie untersucht. Bei der ersten Variante ist der IAA abgeschaltet, also alle *InCo Units* im Szenario aktiv. Wird der IAA verwendet, so werden redundante *InCo Units* deaktiviert. In Abbildung 6.5 sind die drei Szenarien bei Nutzung der prozessintegrieren Ausbrin-



(a) Kleines Szenario (b) Mittleres Szenario (c) Großes Szenario

Abbildung 6.5: Modellierung der Szenarien in OMNeT ohne IAA

gungsstrategie zu sehen. Es ist zu erkennen, dass sehr häufig *InCo Units* platziert wurden. Die Abstände zwischen zwei *InCo Units* entsprechen dabei 20 Metern, also einer Feuerwehr-Schlauchlänge.

Die Summe der angebotenen Datenrate, welche durch die Sender mittels eines konstanten Datenstroms übertragen wird, ist bei der jeweiligen Szenariengröße für beide Positionierungsstrategien gleich. Dies bedeutet, dass beispielsweise im kleinen Szenario und der prozessintegrieren Ausbringungsstrategie die vier Sender mit jeweils 1,5 Mbit/s senden, und im Vergleich dazu die beiden Sender bei der *minRouter* Positionierung mit 3 Mbit/s senden (siehe Tabelle 6.1). Der Grund für die Wahl der Datenrate von 1,5 Mbit/s ist die Paket-Empfangsrate von 100% im kleinen Szenario für beide Protokolle und beide Positionierungsstrategien.

Es wurden zehn Wiederholungen der Untersuchung der Szenarien durchgeführt, wobei jeweils die Positionierungsart (IAA_{aus}, IAA_{an} und *minRouter*) und die Protokolle (BATMAN und OLSR) untersucht wurden. Dazu wurde der Zufallszahlengenerator für jede Untersuchung jeweils neu initialisiert. Für einen fairen Vergleich zwischen BATMAN und OLSR wurden bei beiden Protokollen jeweils die gleichen Zufallszahlen verwendet.

6.3 Leistungsbewertung

Um die Leistungsfähigkeit der im Rahmen dieser Arbeit vorgestellten prozessintegrierten Ausbringungsstrategie für WLAN-Router bewerten zu können, werden zwei Leistungskennzahlen gemessen. Die Paket-Auslieferungsrate (PDR) gibt an, wie viele der versendeten Pakete tatsächlich bei einem Empfänger ankommen. Darüber hinaus gibt die durchschnittliche Verzögerung darüber Auskunft, wie schnell Pakete bei einem Empfänger ankommen.

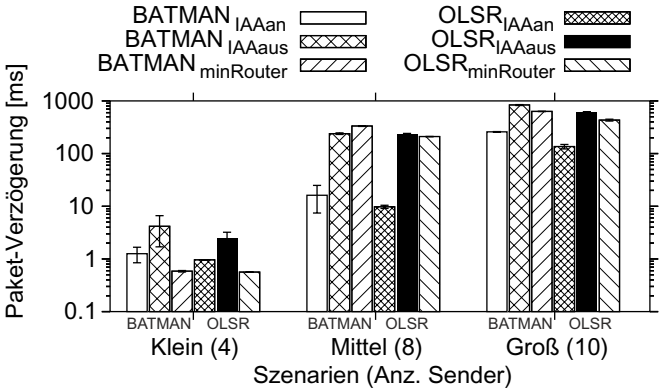


Abbildung 6.6: Durchschnittliche Verzögerung der empfangenen Pakete bei 768 kbit/s angebotenem Verkehr pro Sender

Die durchschnittliche Verzögerung der empfangenen Pakete für alle Szenarien ist in Abbildung 6.6 dargestellt. Sie hängt unter anderem von der Größe des Szenarios ab. Beim kleinen Szenario liefert die *minRouter*-Positionierungsstrategie bessere Ergebnisse als der hier vorgestellte *InCo*-Ansatz. Beim mittleren und großen Szenario führt der *InCo*-Ansatz jedoch zu geringeren Verzögerungen. Dies liegt daran, dass es bei der *minRouter* Strategie aufgrund der höheren Datenrate bei weniger Sendern häufiger zu Kollisionen kommt und daher die IEEE 802.11 DCF zu größeren Verzögerungen zwischen den einzelnen Paketen führt. Dies führt dann zu einer insgesamt höheren durchschnittlichen Verzögerung bei der *minRouter*-Strategie.

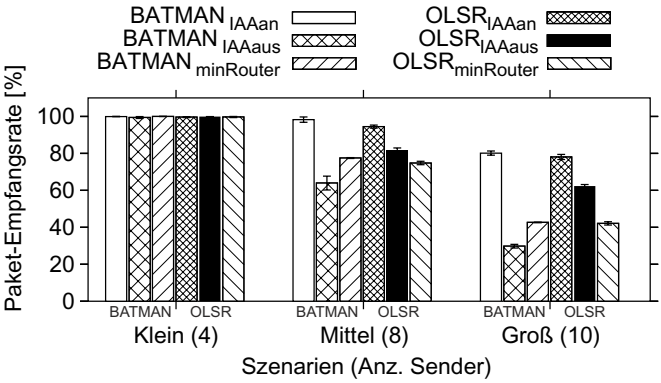


Abbildung 6.7: PDR bei 768 kbit/s angebotenem Verkehr pro Sender

Die PDR für alle Szenarien ist in Abbildung 6.7 dargestellt. Die angebotene Datenrate wurde für alle Szenarien konstant auf 6 Mbit/s konfiguriert, da im kleinen Szenario vier Sender mit jeweils 1,5 Mbit/s senden. Die resultierende PDR ist in Abbildung 6.7 dargestellt. Das Ergebnis zeigt, dass BATMAN unabhängig von der Szenariengröße und der Positionierungsstrategie etwas bessere PDRs liefert als OLSR. Wie weiter oben erwähnt, wurde der Verkehr so gewählt, dass der PDR im kleinen Szenario bei beiden Positionierungsstrategien 100% erreicht. Im mittleren Szenario erreicht das Interkupplungskonzept mit aktivem IAA und BATMAN eine PDR von nahezu 100%. Bei der Verwendung von OLSR wird nur geringfügig weniger PDR erreicht. Das Ergebnis der *minRouter*-Positionierung ist jedoch etwas schlechter. Bei der Verwendung von BATMAN wird ein PDR von ca. 80% und bei OLSR von ca. 75% erreicht.

Auch im großen Szenario ist das Ergebnis des Interkupplungskonzepts ca. 15% besser als das Ergebnis der *minRouter*-Positionierung. Insgesamt ist die Paket-Empfangsrate im großen Szenario geringer als im kleinen und mittleren Szenario.

Zur Begründung der Ergebnisse sei auf die steigende Anzahl von Paketen bei steigender Szenariengröße aufgrund der steigenden Anzahl von Sendern hingewiesen. Es wird erwartet, dass die PDR mit steigender Szenariengröße sinkt, da mehr Kollisionen auftreten werden. In diesem Kontext sei noch einmal darauf hingewiesen, dass bei der *minRouter*-Positionierungsstrategie die minimale Anzahl von verwendeten Routern im Vordergrund stand. Diese minimale Anzahl von Routern und ein hoher angebotener Verkehr, der verteilt von sechs Sendern an einen Empfänger fließt, welcher im Zentrum des Szenarios positioniert ist, kann zu einer Überlastung der DCF-Warteschlange führen. Aufgrund der redundanten Routen, die bei der Verwendung des hier vorgestellten Interkupplungskonzepts auftreten, ist das Interkupplungskonzept bei dem Hochlastszenario effizienter als die *minRouter*-Positionierungsstrategie.

6.4 Experimentelle Validierung im Feldtest bei der Feuerwehr

Nachdem die Funktionalität des Vernetzungskonzepts mittels einer Simulation überprüft wurde, wird nun mit Hilfe der prototypischen Umsetzung der *Dropped Units* eine experimentelle Validierung im Feldtest bei der Feuerwehr Gelsenkirchen vorgestellt. Die Feuerwehr besitzt ein so genanntes Brandhaus, welches zu Trainingszwecken angezündet werden kann. Es besteht aus Stahlbeton und ist im Inneren mit Möbeln aus Edelstahl ausgestattet. Um Teile des Hauses in Brand zu setzen, wird Gas eingeströmt und verbrannt. Das Brandhaus hat annähernd die Grundfläche eines normalen Einfamilienhauses (siehe Abbildung 6.8).

Für die experimentelle Untersuchung wurde ein Einsatzleitfahrzeug in der Nähe der Halle geparkt und mit einem WLAN-*Access Point* ausgestattet. Anschließend wurde mit einem Laptop und dem Programm *ping* überprüft, in welchen Bereichen

Abbildung 6.8: Brandhaus der Feuerwehr Gelsenkirchen

der WLAN-Empfang noch möglich war. Dabei wurde das Brandhaus in ähnlicher Weise umrundet, wie ein Erkunder es bei der Halle aus der Simulation getan hätte. Auch beim Experiment ist der WLAN-Empfang an den vom ELW abgewandten Gebäudeseiten so schlecht, dass die Kommunikation abgebrochen ist. Anschließend wurden *Dropped Units* an den Gebäudeecken platziert. Daraufhin war eine Kommunikation mit dem ELW wieder möglich.

6.4.1 Prozessorientiertes Interkupplungskonzept

Bei dem Feldtest in Gelsenkirchen wurden im Wesentlichen zwei Tests durchgeführt. Zunächst wurde das Interkupplungskonzept überprüft. Bei diesem Test geht es um die Untersuchung der Videoübertragung von einer am Helm eines Feuerwehrmanns befestigten Kamera zu dem im ELW befindlichen Einsatzleiter mittels WLAN. Solange sich der Feuerwehrmann in der Nähe des ELWs befindet und sich kein Hindernis in der Sichtverbindung befindet funktioniert die Videoübertragung störungsfrei. Diese Situation ist in Abbildung 6.9 zu sehen. Betritt der Feuerwehrmann ein Gebäude, so bricht die Videoübertragung ab. Um dies zu verhindern, werden *InCo Units* in die Kupplung der Feuerwehrschläuche eingebracht. Somit wird beim Ausbringen des Schlauches jede 20 Meter ein WLAN-Router abgelegt.

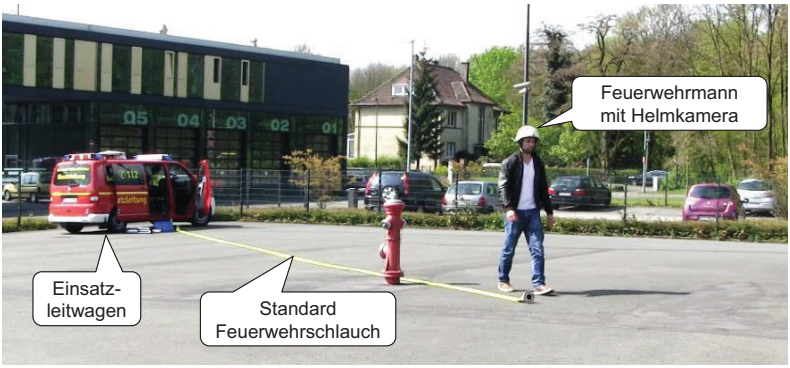


Abbildung 6.9: Videoübertragung von einer Helmkamera zum ELW

In dem hier beschriebenen Feldtest wurde untersucht, ob die Videoübertragung aus einem Gebäude zum ELW über mehrere *InCo Units* funktioniert. Dabei wurden zwei Strategien miteinander verglichen. Zunächst wurde ein Feuerwehrschlauch verwendet, um alle 20 Meter eine *InCo Unit* zu platzieren. Wird diese Strategie verwendet, so werden vier *InCo Units* für die Kommunikation benötigt. Zusätzlich zu drei in den Schlauchkupplungen positionierten *InCo Units* wird eine weitere *Dropped Unit* hinter dem Eingangsbereich benötigt (vgl. Abbildung 6.10). Dieser Mehraufwand ist für die Rettungskräfte keine große Belastung, weil sie sich zur Regel machen können, an jedem Hauseingang, den sie passieren, eine *Dropped Unit* aufzustellen.

Abbildung 6.10: DU am Eingang

Werden die *InCo Units* frei positioniert, kann die benötigte Zahl auf 3 reduziert werden. Zwar wird bei dieser Strategie eine *InCo Unit* weniger benötigt, aber dafür müssen die Feuerwehrleute mehr Aufwand betreiben, um das Netz aufzubauen.

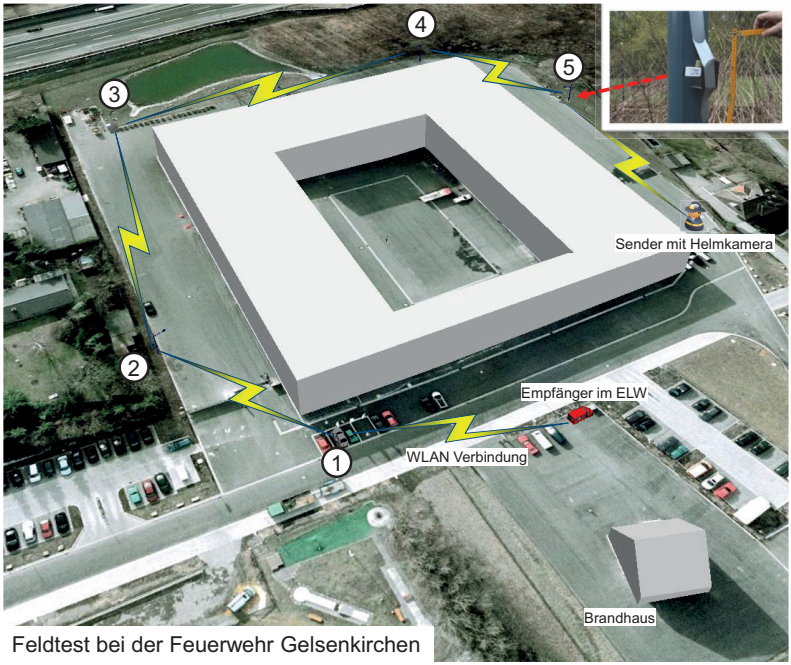


Abbildung 6.11: Feldtest zur Videoübertragung bei großen Entfernungen bei der Feuerwehr Gelsenkirchen

6.4.2 Audiovisuelle Positionierung

Ein weiterer Feldtest untersucht die Kommunikationsqualität bei großen Entfernungen, wobei die WLAN-Router in Form von *Dropped Units* mittels der audiovisuellen Positionierung durch einen Erkunder manuell positioniert werden (vgl. Kapitel 3.5). Um große Entfernungen überbrücken zu können, werden viele *InCo Units* bzw. *Dropped Units* benötigt. Es wurde untersucht, ob eine Videoübertragung auch bei großen Entfernungen, also der Verwendung von 5 *Dropped Units*, noch den Anforderungen entsprechend funktioniert. In Abbildung 6.11 ist der Messaufbau an der Hauptwache der Feuerwehr Gelsenkirchen dargestellt.

Der Erkunder, der mit einer Helmkamera ausgestattet ist, startet zunächst am ELW und umrundet anschließend das Hauptgebäude. Immer, wenn der Empfang schwach wird, platziert er eine *Dropped Unit*. Um die in Kapitel 3.3 untersuchte minimale Antennenhöhe einzuhalten, wurden die *Dropped Units* in ca. 1,5 m Höhe an Laternenmasten befestigt.

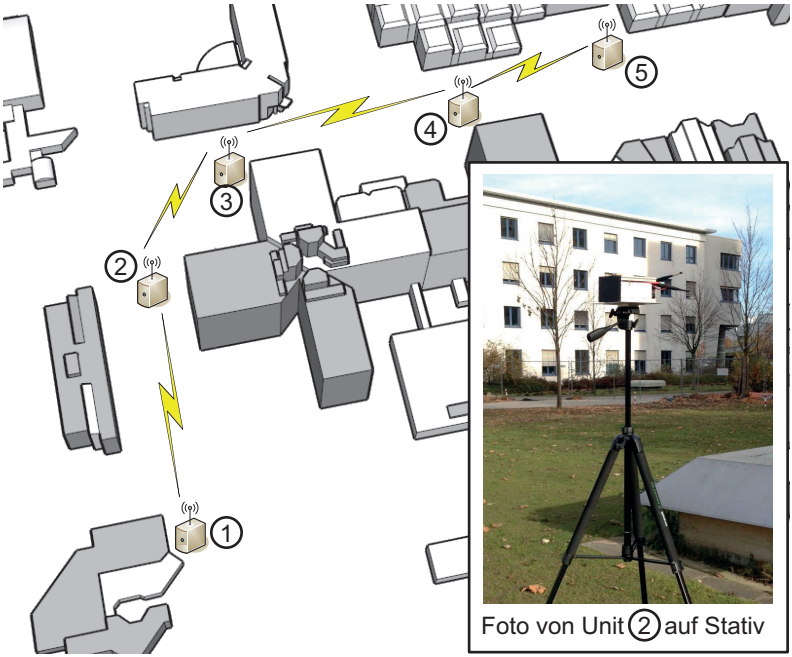
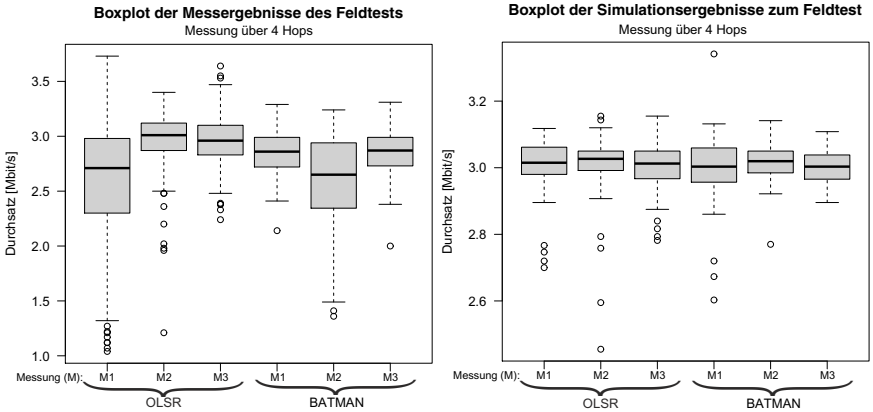


Abbildung 6.12: Positionen der *Dropped Units* für den Feldtest an der TU

Der Empfang des Videos wurde permanent durch einen Zuschauer im ELW überwacht. Immer wenn der Empfang schlechter wurde hat der Zuschauer über Sprechfunk dem Erkunder Bescheid gegeben, damit dieser eine *Dropped Unit* platziert. So ist eine Übertragung komplett um das Gebäude herum möglich. An der Endposition wurde darüber hinaus eine kurze Durchsatzmessung mittels iPerf durchgeführt. Innerhalb des Messzeitraums von 20 Sekunden schwankte der ermittelte Durchsatz zwischen 1,05 Mbit/s und 2,1 Mbit/s.

Für eine detailliertere Untersuchung wurde die Messung am Campus der TU Dortmund wiederholt. Die Positionen der *Dropped Units* sind in Abbildung 6.12 dargestellt, wobei jede *Dropped Unit* auf einem 1,5 m hohen Stativ montiert wurde. Zwischen den am weitesten entfernten *Dropped Units* (Nr. 1 und Nr.5 in der Abbildung) wurde der Durchsatz mittels iPerf ermittelt. Für die Vernetzung sind die Routing-Protokolle OLSR und BATMAN eingesetzt worden. Jede Messung hatte eine Dauer von 3 Minuten und wurde drei Mal wiederholt.

Die Ergebnisse des Feldtests sind in Abbildung 6.13(a) als Boxplot Diagramm dargestellt. Jeder Boxplot repräsentiert die iPerf Ergebnisse einer Messung von 180 Sekunden Dauer, wobei der Durchsatz einmal pro Sekunde ermittelt wurde.



(a) Auswertung des Feldtests (b) Auswertung der Simulation

Abbildung 6.13: Ergebnisvergleich Feldtest mit Simulation

Die Messungen wurden im Abstand von wenigen Minuten durchgeführt, wobei die gesamte Teststrecke nicht komplett überwacht wurde. Die Schwankungen in den Messergebnissen können somit durch Fußgänger auf dem Campus verursacht worden sein. Diese Schwankung kann besonders bei Messung 1 von OLSR und Messung 2 von BATMAN beobachtet werden.

Der Einfluss des Routing-Protokolls ist in diesem Szenario gering. Dies ist daran zu erkennen, dass sich die Ergebnisse der beiden Protokolle OLSR und BATMAN kaum voneinander unterscheiden. Lässt man Messung 1 von OLSR und Messung 2 von BATMAN außer Acht, so erreicht OLSR einen minimal besseren Durchsatz von ca. 3 Mbit/s im Vergleich zu BATMAN, welches ca. 2,8 MBit/s im Durchschnitt erreicht.

Zusätzlich wurde der Feldtest in der weiter oben beschriebenen Simulationsumgebung modelliert. Die Ergebnisse der simulativen Untersuchung sind in Abbildung 6.13(b) als Boxplots dargestellt. Im Vergleich zur realen Messung im Feld ist die Streuung der Ergebnisse in der Simulation wie erwartet geringer. Der Unterschied zwischen den beiden Protokollen BATMAN und OLSR ist bei den betrachteten Szenario vernachlässigbar. Es wird bei beiden Protokollen ein Durchsatz im Durchschnitt von ca. 3 Mbit/s erreicht.

In den hier untersuchten Szenarien hat sich gezeigt, dass die Anforderungen der Rettungskräfte an das Kommunikationsnetz durch den Einsatz der *Dropped Units* erfüllt wird. Die erreichbare Datenrate reicht aus, um Videos von einer Helmkamera über mehrere Hops zu einem entfernten Empfänger zu übertragen. Insgesamt sind die Feldtests bei der Feuerwehr Gelsenkirchen und am Campus der TU

Dortmund sehr positiv verlaufen. Die beteiligten Feuerwehrbeamten sind von dem Ergebnis überzeugt und können sich vorstellen, die Technologie auch im Einsatzfall einzusetzen. Die Verwendung von Videoübertragungen von den Helmkameras zum ELW würde die Arbeit der Einsatzleiter erleichtern und stellt eine sinnvolle Ergänzung zum bisherigen Prozess dar.

6.5 Zusammenfassung

Im Rahmen der hier vorgestellten Leistungsbewertung wurde der neue prozessintegrierte Ausbringungsansatz, bei dem die Aufgabe des Kommunikationsnetzaufbaus in den Rettungsprozess mittels Integration von *InCo Units* in Feuerwehrschläuche gelöst wird, mit einer Positionierungsstrategie verglichen, bei der die optimierten Positionen von WLAN-Routern von vornherein berechnet werden. Der neue prozessintegrierte Ausbringungsansatz hat zum Ziel, einen möglichst komfortablen Weg für die Rettungskräfte aufzuzeigen, um ohne zusätzlichen Arbeitsaufwand ein Ad-hoc-Netz aufzubauen. In der Regel wissen Rettungskräfte nicht, wo sich die optimalen Positionen für WLAN-Router an einem Einsatzort befinden, und sie haben auch nicht die Zeit, die WLAN-Router an speziell dafür ausgewählten Orten aufzustellen. Daher ist der hier vorgestellte prozessintegrierte Ansatz für Rettungskräfte einfacher anzuwenden und zum Rettungsprozess konform. Darüber hinaus können die *InCo Units* nach Einsatzende einfach eingesammelt werden, indem der Feuerwehrschlauch eingeholt wird.

Die Leistung des prozessorientierten Interkupplungskonzepts wurde mit einer Strategie verglichen, die auf einem minimalen Steinerbaum-Ansatz beruht. Es wurden drei unterschiedliche Szenarien und zwei Routing-Protokolle, BATMAN und OLSR, untersucht. Die Ergebnisse zeigen, dass das im Rahmen dieser Arbeit vorgestellte Interkupplungskonzept vergleichbare Ergebnisse zu der *minRouter*-Positionierungsstrategie im kleinen und mittleren Szenario liefert. Im großen Szenario ist der neue Ansatz im Hinblick auf die PDR sogar etwas besser. Somit bietet das Interkupplungskonzept eine komfortable Lösung, um ein Kommunikationsnetz bei Großschadenslagen aufzubauen.

In den abschließenden experimentellen Untersuchungen wurde neben dem Interkupplungskonzept auch die audiovisuell unterstützte Platzierung untersucht. Es konnte gezeigt werden, dass das Interkupplungskonzept für die Vernetzung von Rettungskräften bei einem Hausbrand eingesetzt werden kann. Darüber hinaus konnte gezeigt werden, dass mittels der audiovisuell unterstützten Positionierung auch ein weit von einem Empfänger entfernter Sender noch ein Helmkameravideo über das Ad-hoc-Netz übertragen kann.

7

Zusammenfassung, Fazit und Ausblick

Die Zusammenfassung greift die wichtigsten Themen der Arbeit auf und geht kurz auf diese ein. Das Fazit ordnet die Arbeit in einen größeren Kontext ein und zeigt, dass sich das Thema Ad-hoc-Vernetzung auf breiter Ebene durchsetzt. Dazu wird ein aktuelles Projekt vorgestellt, bei dem die im Rahmen dieser Arbeit erforschten Konzepte zum Tragen kommen. Schließlich wird im Ausblick eine mögliche Verwertung der Ergebnisse der vorliegenden Arbeit beschrieben.

7.1 Zusammenfassung

Im Rahmen dieser Arbeit wurden ein Ad-hoc-Vernetzungskonzept vorgestellt, welches von Rettungskräften am Einsatzort eingesetzt werden kann. Bei der Diskussion über dieses Vernetzungskonzept mittels *Dropped Units* sind Hindernisse aufgedeckt worden, welche die Rettungskräfte möglicherweise in ihrem Handeln am Einsatzort stören. Um diese Hindernisse auszuräumen, wurde ein neuartiger, prozesskonformer Netzaufbau vorgeschlagen. Hierbei werden die *Dropped Units* nicht mehr manuell an bestimmten Orten ausgelegt, sondern *on-the-fly* ausgebracht, da sie in die Schlauchkupplungen von Feuerwehrschläuchen integriert sind. Dieser neue Lösungsansatz wird sowohl mittels simulativer Experimente, als auch mit Hilfe eines Messaufbaus evaluiert. Es zeigt sich, dass die Verwendung des neuen, prozesskonformen Netzaufbaus zu ähnlichen Ergebnissen führt wie die Platzierung der *Dropped Units* an bestimmten Positionen. Eine Einschränkung hat das neue Konzept jedoch: Es führt zu einer Überbelegung eines Szenarios mit redundanten *InCo-Units*. Daher wurde ein neuartiger Interferenz-Vermeidungs-Algorithmus erforscht, der die redundanten *InCo Units* deaktivieren kann. Schließlich wird ein neues Konzept zur Realisierung von Dienstgüte vorgestellt, welches speziell auf die Bedürfnisse von Rettungskräften im Katastrophenschutz ausgelegt ist. Diese Realisierung der Dienstgüte basiert auf einer Modifikation der IEEE 802.11 DCF unter Anlehnung an den IEEE 802.11e. Die Leistungsfähigkeit der Dienstgüte wird anhand analytischer und simulativer Modelle untersucht. Dieses abschließende Kapitel gibt eine Zusammenfassung der durchgeführten Arbeiten und Ergebnisse im Hinblick auf die Optimierung der verschiedenen Themenkomplexe dieser Arbeit. Ferner wird ein Ausblick auf mögliche Folgearbeiten gegeben.

7.1.1 Prozess-integrierte Ad-hoc-Vernetzung

Um neuartige Dienste, wie beispielsweise die Übertragung eines Live-Videos von einer Helmkamera, bei einer Großschadenslage zu ermöglichen, wird ein ausfallsicheres Kommunikationsnetz benötigt. In Kapitel 3 wird das im Rahmen dieser Arbeit entstandene Konzept vorgestellt. Es basiert im Wesentlichen auf dem Einsatz von *Dropped Units*, also batteriebetriebener WLAN-Router.

Durch eine Abdeckungsanalyse konnte gezeigt werden, dass schon wenige *Dropped Units* ausreichen, um das Gebiet um und in einer kleinen Lagerhalle (10m · 10m) mit WLAN zu versorgen. Es konnten einfache Ausbringungsregeln abgeleitet werden, die den Rettungskräften am Einsatzort die Positionierung der *Dropped Units* erleichtern. Beispielsweise sollen *Dropped Units* an Durchgängen bzw. Türen und an Gebäudeecken positioniert werden, da dort häufig die Sichtverbindung zur vorherigen *Dropped Unit* unterbrochen wird.

Darüber hinaus wurde ein neues Konzept zur Positionierung von WLAN-Routern vorgestellt, welches zum Ziel hat, Rettungskräfte beim Aufbau eines Ad-hoc-Netzes zu unterstützen, ohne sie bei ihrer eigentlichen Tätigkeit zu behindern. Im Vordergrund stand dabei ein Konzept, bei der die Technik der Taktik folgen soll. Im Rahmen dieser Arbeit wurden *InCo Units* vorgestellt, welche zwischen Feuerwehrschläuche gekoppelt werden. Dadurch wird jeder zusätzliche Arbeitsaufwand vermieden, um das Kommunikationsnetz für die Rettungskräfte aufzubauen.

7.1.2 Algorithmen zur Interferenzreduktion

Der in Kapitel 4 vorgestellte Interferenz-Vermeidungs-Algorithmus (IAA) sorgt dafür, dass die redundant positionierten *InCo Units* die Kommunikation nicht stark beeinflussen. So ist die Anzahl der benötigten *InCo Units* in kleinen und mittleren Szenarien nur geringfügig höher als bei der Positionierung der WLAN-Router an zuvor mittels optimierenden Algorithmen berechneten Orten. Wird berücksichtigt, dass Feuerwehrleute im Normalfall nicht wissen, wo sich die optimalen Orte für WLAN-Router befinden, und ihnen keine Zeit zur Verfügung steht, um sie gesondert abzulegen, stellt das hier vorgestellte *InCo Units*-Konzept in Kombination mit dem IAA eine einfache Lösung zur Vernetzung der Rettungskräfte dar, welches sich leicht in den Rettungsprozess integrieren lässt.

7.1.3 Dienstgüte für den Katastrophenschutz

In Kapitel 5 wurde ein neuer Parametersatz für die DCF vorgestellt, welcher Dienstgüte in Szenarien für den Katastrophenschutz ermöglicht. Dieser Parametersatz wird *Emergency-DCF* (EDCF) genannt. Es werden sechs neue Zugriffskategorien definiert, welche für die unterschiedlichen Kommunikationsarten im Kata-

strophenschutz stehen. Dabei werden alle neuen Kommunikationsarten gegenüber ursprünglicher IEEE 802.11-Kommunikation priorisiert übertragen. Für die Leistungsbewertung der EDCF wurde ein existierendes Markov-Modell angepasst und erweitert. Anhand dieses erweiterten Modells wurde dann der Sättigungsdurchsatz analysiert. Die analytisch ermittelten Ergebnisse wurden schließend mittels einer Simulation verifiziert. Es wurden zwei Szenarien analysiert: Im ersten Szenario wurde überprüft, ob EDCF-Nutzer immer einen höheren Sättigungsdurchsatz erzielen als ursprüngliche IEEE 802.11-Nutzer. Das zweite Szenario untersucht die Dienstgüte-Unterstützung der EDCF. Dabei wird der Sättigungsdurchsatz von zwei unterschiedlichen Zugangskategorien untersucht. Die Ergebnisse der Leistungsbewertung zeigen, dass der hier vorgeschlagene Parametersatz eine zuverlässige Kommunikation in den untersuchten Katastrophenschutz-Szenarien ermöglicht. Dies gilt selbst dann, wenn ursprüngliche WLAN-Netze am Einsatzort existieren.

7.2 Fazit

Gerade im Katastrophenschutz lassen sich Ad-hoc-Netze sinnvoll einsetzen. Wenn Infrastrukturnetze überlastet oder zerstört sind, müssen Rettungskräfte ihr eigenes Kommunikationsnetz aufbauen. Der Aufbau sollte dabei die Rettungskräfte möglichst nicht behindern. Der im Rahmen dieser Arbeit vorgestellte praxisorientierte Interkupplungsansatz zeigt dabei einen Weg, wie ein Ad-hoc-Netz „on-the-fly“ aufgebaut werden kann.

Der Einsatz von Ad-hoc-Netzen in vielen Forschungsprojekten zeigt, dass das Thema eine hohe Relevanz aufweist. Es kann davon ausgegangen werden, dass auch zukünftig nach Prozessen gesucht wird, die den praxisnahen Aufbau eines Ad-hoc-Netzes ermöglichen.

Bei der Kommunikation im Katastrophenschutz müssen sich die Rettungskräfte auf das Kommunikationsnetz verlassen können. Die im Rahmen dieser Arbeit vorgestellte „audiovisuell unterstützte Platzierung“ und das „Interkupplungskonzept“ stellen zwei Ansätze dar, wie ein solches Ad-hoc-Netz aufgebaut werden kann. Darüber hinaus wird mittels der „Emergency-DCF“ eine Priorisierung vorgenommen und mittels des „*Interference Avoidance Algorithm*“ die Selbststörung durch redundante WLAN-Router vermieden. Insgesamt kann zusammenfassend gesagt werden, dass die Anforderungen der Rettungskräfte durch die neuen Ansätze erfüllt werden.

Die im Rahmen dieser Arbeit erarbeiten Verfahren werden aktuell in Kooperation mit dem DRK in Bayern im Einsatz erprobt. In dem gemeinsamen Projekt *RescueNet* werden *Dropped Units* in spritzwassergeschützten Gehäusen eingesetzt, die an einem Einsatzort auf Stativen verteilt werden. Als Eingebettetes System wird in den *Dropped Units* des *RescueNet* ein *Raspberry Pi* eingesetzt, der nochmals

eine Kostenersparnis für den Endanwender darstellt. Das DRK in Bayern kommuniziert in der Regel Statusmeldungen, wie z.B. die Behandlungsplatzkapazität oder die Anzahl der bisher behandelten Patienten, per Sprechfunk. Durch den Einsatz von IP-basierten Diensten kann der ressourcenbeschränkte Sprechfunkkanal entlastet werden. Dies zeigt den praktischen Nutzen der im Rahmen dieser Arbeit erarbeiteten Konzepte.

7.3 Ausblick

Das im Rahmen dieser Arbeit entstandene prozessintegrierte Konzept zum Netzaufbau sollte weiter untersucht werden. Hier ist insbesondere zu prüfen, wie mögliche Lücken in der Funkfeldabdeckung geschlossen werden können, ohne die Rettungskräfte mit zusätzlicher Arbeit zu belasten. Bei Experimenten mit der Feuerwehr hat es sich gezeigt, dass insbesondere Hauseingänge Hindernisse darstellen, die mit dem Schlauchkonzept nur gerade noch ausreichend überbrückt werden können. Eine erste Idee, dieses Problem zu lösen, ist ein verschiebbarer Ring, der am Schlauch befestigt und in den Türbereich verschoben wird. Dieser Ring kann aus einer Art Klettverschluss bestehen, in den die drei Komponenten der hier vorgestellten *InCo Units* eingearbeitet sind. So kann ein solcher Ring bei Bedarf schnell am Schlauch befestigt und positioniert werden.

Für den Ad-hoc-Netzaufbau können zusätzlich zu den *Dropped Units* und den *InCo Units* autonome Flugroboter eingesetzt werden. Hier wäre nur wenig Mehrarbeit für die Rettungskräfte von Nöten. Im Projekt Airshield wurde eine GUI entwickelt, die es erlaubt, einen Bereich in einer Karte einzuzeichnen, der anschließend von Flugrobotern abgedeckt wird. Die Einschränkung der Machbarkeit besteht aber bisher darin, dass die Flugzeit der Flugroboter aufgrund des begrenzten Akkus viel geringer ist als die Einsatzdauer bei einer Großschadenslage. Hier setzt das Projekt AVIGLE an [69], bei dem ein *tilt-wing - remotely piloted vehicle*, kurz TW-RPV, erforscht wird. Das TW-RPV-Konzept spart durch den Gleitflug im Vergleich zum Quadrocopter Energie ein, die bei gleicher Akku-Dimensionierung für längere Flugdauern genutzt werden kann.

Die im Rahmen dieser Arbeit vorgestellte Ad-hoc-Vernetzung mittels WLAN, die eine hohe Datenrate am Einsatzort bietet, hat eine begrenzte Reichweite. Um diese zu erweitern, können zukünftig LTE-basierte Systeme eingesetzt werden, wie im Projekt Anchors [42] vorgeschlagen wurde. In Anchors werden Flugplattformen mit einem ferngesteuerten „Mobilen Transport System“ (MTS) in die Nähe eines Einsatzortes, der für Menschen unzugänglich ist, gebracht. Die Daten der Flugroboter werden dann entweder per WLAN-Ad-hoc-Netz oder per LTE an eine Leitstelle übertragen. Die im Rahmen dieser Arbeit vorgestellte Ad-hoc-Vernetzung stellt somit eine kostengünstige Übergangslösung hin zu einem kombinierten Vernetzungskonzept mittels heterogener Kommunikationstechnologien dar.

Ein weiterer Aspekt dieser Arbeit, der in Zukunft weiter untersucht werden kann, ist die Unterstützung von Dienstgüte für die WLAN-Kommunikation am Einsatzort. Im Rahmen dieser Arbeit wurde eine Grundlage gelegt, auf die nun aufgebaut werden kann. Unter anderem ist zu untersuchen, wie die unterschiedlichen Dienste auf die Zugriffskategorien zugreifen können. Hier gilt es eine Metrik zu erforschen, welche die Dienste anhand bestimmter Merkmale bestimmten Zugriffskategorien zuordnen kann. Ferner wird sich die Frage stellen wie die unterstützte Gruppengröße erhöht werden kann. Darüber hinaus sind alternative Priorisierungsmethoden denkbar, die es zu untersuchen gilt.

In Kooperation mit dem Bayerischen Roten Kreuz konnten die *Dropped Units* auf dem 8. Bayerischen Katastrophenschutz-Kongress einem breiten Fachpublikum vorgestellt werden. Ermunternd für die weitere Entwicklung war dabei das Interesse des Bundesinnenministeriums an dem System. Dadurch wurde auch die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) aufmerksam und ist an der weiteren Entwicklung interessiert.

A

Ad-hoc-Vernetzung für den Katastrophenschutz im Kontext von Forschungsprojekten

Nachfolgend wird der Einsatz von Ad-hoc-Kommunikationsnetzen für den Katastrophenschutz im Kontext einiger ausgewählter Projekte dargestellt. Dabei werden sowohl eigene Projekte vorgestellt als auch Projekte ohne Beteiligung des Autors, welche jedoch in den gleichen Kontext einzuordnen sind.

A.1 Projekte des Lehrstuhls mit eigener Beteiligung

A.1.1 Airshield

Im Rahmen des vom BMBF geförderten Projektes Airshield wird ein Ad-hoc-Netz für die Kommunikation und Koordination von Flugrobotern eingesetzt. In Airshield messen Flugroboter mit Hilfe von speziellen Sensoren den Schadstoffgehalt der Luft. Die Airshield-Quadrocopter sind in Abbildung A.1 dargestellt. Um eine Schadstoffquelle zu lokalisieren, wird nicht nur ein Flugroboter eingesetzt, sondern ein ganzer Schwarm von Flugrobotern, welcher die Schadstoffquelle anhand des Konzentrationsgefälles eingrenzen kann. Für eine erfolgreiche Zusammenarbeit der Flugroboter im Schwarm ist ein Datenaustausch zwischen den Flugrobotern zwingend erforderlich. Dies ist nicht nur für die Lokalisation der Schadstoffquelle notwendig, sondern auch für die Kollisionsvermeidung. Darüber hinaus wird eine Kommunikation mit einer Bodenstation ebenfalls benötigt, da der autonome Schwarm seine Befehle von einem Benutzer am Boden erhält. Dafür wird die Bodenstation ebenfalls Teil des Ad-hoc-Netzes. Zudem muss der Datenaustausch, mit Rücksicht auf die Fluggeschwindigkeit der Flugroboter, nahezu in Echtzeit ablaufen. Wird zusätzlich zu den Schadstoffmessungen ein Video von den Flugrobotern an den Boden gesendet, so muss auch auf die dafür erforderliche Datenrate geachtet werden.

Für die Realisierung des Ad-hoc-Netzes in Airshield wurden dieselben Komponenten eingesetzt, die auch für die im Rahmen dieser Arbeit vorgestellten *Dropped*

Abbildung A.1: Airshield Quadrocopter

Units benutzt wurden. Somit konnten die mit den *Dropped Units* gesammelten Erfahrungen direkt in das Airshield-Projekt einfließen. Unter anderem wurde auch das 5 GHz Band verwendet, um Interferenzen, die durch andere WLAN Stationen im 2,4 GHz verursacht werden könnten, zu vermeiden.

Airshield stellt einen Dienst bereit, welcher auf Basis von in der Luft gemessener Schadstoffwerte, eine Vorhersage über die Schadstoffintensität und den Ort des Niedergangs einer Rauchwolke trifft. Die Schadstoffmessung wird mit Hilfe von autonom agierenden Quadrocoptern vorgenommen, die mittels des WLAN Ad-hoc-Netzes ständig die gemessenen Schadstoffwerte und Positionsdaten austauschen. Darüber hinaus werden die Daten an eine Bodenstation gesendet, welche sie weiter verarbeitet. Die Airshield-Architektur ist in Abbildung A.2 dargestellt.

Das Airshield System lässt sich grob in zwei Bestandteile gliedern. In der Luft sammelt der Schwarm zunächst die Messdaten. Diese werden dann an das GIS-System am Boden gesendet. Das GIS-System am Boden wertet die Messdaten aus und steuert kontextsensitiv den Schwarm. Weitere Informationen zum Airshield System finden sich in [15].

Bei einem abschließenden Systemtest bei dem Rotterdam International Safety Center (RISC), einem internationalen Trainings- und Übungszentrum für Feuerwehren, konnte die Funktionsfähigkeit des Ad-hoc-Kommunikationsnetzes unter extremen Bedingungen erfolgreich getestet werden.

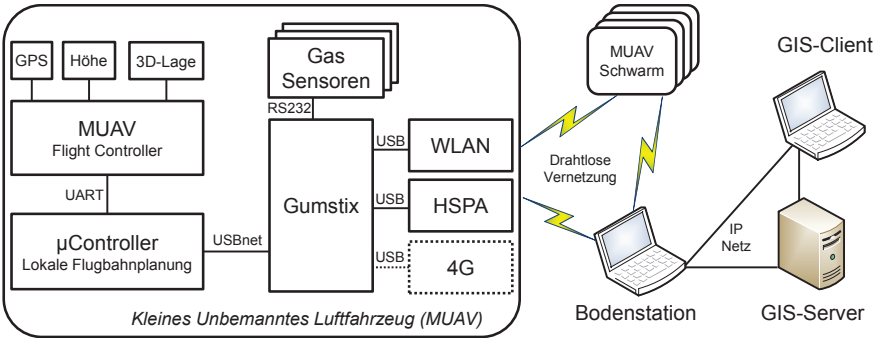


Abbildung A.2: Airshield Architektur

A.1.2 SPIDER

Im Projekt *Security System for Public Institutions in Disastrous Emergency scenaRios* (SPIDER) wird das Ad-hoc-Netz für die Vor-Ort Kommunikation der Rettungskräfte eingesetzt. Wesentlicher Vorteil ist dabei, dass Informationen zu Verletzten nur noch einmal aufgenommen werden müssen. Im Feld kann beim Erstkontakt mit einem Verletzten eine Datenaufnahme durchgeführt werden, die anschließend von allen an der Rettungskette beteiligten Organisationen und Einrichtungen abgerufen werden kann. Somit wird Rettungskräften bei Großschadensfällen ein ganzheitliches, intelligentes Kommunikations- und Informationssystem zur Verfügung gestellt. Dadurch wird allen Beteiligten ein effizientes Notfall-Prozessmanagement ermöglicht.

Die behördliche Koordination aller Hilfs- und Rettungsmaßnahmen stellt eine große Herausforderung dar, sobald mehrere hundert Verletzte medizinisch und psychologisch versorgt werden müssen. Gleichzeitig ist eine Masse von Informationen zu bewältigen, wobei sehr unterschiedliche Organisationen wie Polizei, Feuerwehr, Rettungsdienst, diverse Hilfsorganisationen, Notärzte, Notfallseelsorger, KITs (Krisenintervention im Rettungsdienst) zusammen arbeiten.

Organisationsspezifische Informationssysteme sind zwar verfügbar, doch arbeiten die Systeme der Institutionen heutzutage nur marginal vernetzt zusammen. Vorhandene Informationssysteme aus dem Bereich des Gebäudemanagements (Facility Management) sind dabei für die Einsatzkräfte ebenso wenig verfügbar. Dies erschwert zum einen die Rettung von Verletzten und zum anderen den Ad-hoc-Aufbau der Notfalllogistik, da der akute Bedarf schwer abgeschätzt werden kann. Darüber hinaus könnten weitere Rettungsmittel im Rahmen der überörtlichen Hil-

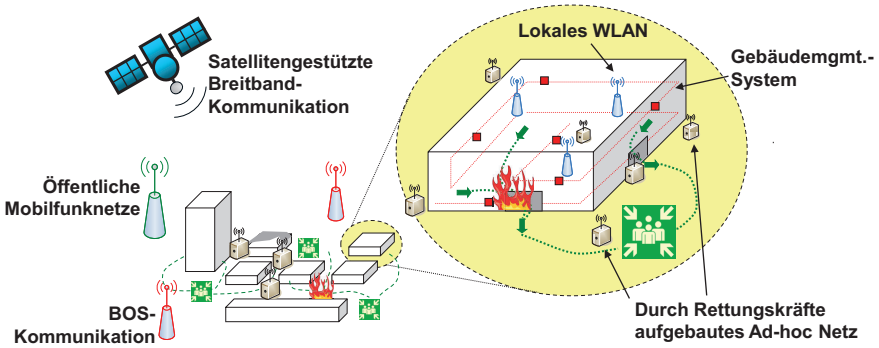


Abbildung A.3: Schutz- und Rettungsszenario in SPIDER [98]

fe angefordert werden. Erschwert wird die Situation einer Großschadenslage weiterhin dadurch, dass Kommunikationssysteme, wie der zellulare Mobilfunk, eventuell ausfallen oder aufgrund von Überlastung nicht genutzt werden können. Das Schutz- und Rettungsszenario, welches in SPIDER adressiert wird, ist in Abbildung A.3 dargestellt.

Der Datenaustausch im Föderationssystem erfolgt über ein übergreifendes Datenaustauschformat. Die *Protection and Rescue Markup Language* (PRML) ermöglicht ein föderiertes Informations- und Kommunikationssystem aller beteiligten Schutz- und Rettungsorganisationen.

Aufgrund der sensiblen Daten im Föderationssystem von SPIDER, wird sowohl für die Vernetzung der Einsatzkräfte vor Ort, als auch für die Weitverkehrsvernetzung der Organisationen eine hochzuverlässige Kommunikationsinfrastruktur benötigt. Der Aufbau des Ad-hoc-Netzes in SPIDER wird durch die im Rahmen dieser Arbeit vorgestellten *Dropped Units* realisiert. In der Regel wird dabei die audiovisuell unterstützte Platzierung (AVUP) eingesetzt.

Falls jedoch ein Feuer bei der Großschadenslage ausgebrochen ist, so wird der praxisorientierte Ansatz des Schlauchkupplungskonzepts eingesetzt. Dabei wird der Feuerwehr ein integrierter Aufbau des Ad-hoc-Netzes „on-the-fly“ ermöglicht. Die Leistungsbewertung der in SPIDER eingesetzten vor Ort Vernetzung wurde im Rahmen der vorliegenden Arbeit durchgeführt.

A.1.3 MORE - Eine Middleware für eingebettete Systeme

Das MORE Projekt (engl. Network-centric Middleware for Group communication and Resource Sharing across Heterogeneous Embedded Systems) hat zum Ziel eine

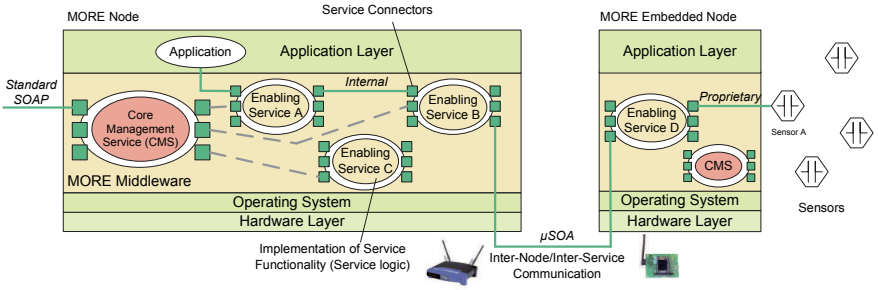


Abbildung A.4: MORE Gesamtarchitektur [97]

Middleware für Eingebettete Systeme zur Verfügung zu stellen, um Anwendungsentwicklern die Möglichkeit zu geben, auf einfache Weise neuartige Dienste für eingebettete Systeme zu implementieren. Ein Ad-hoc-Netz wird im Kontext von MORE für die Vernetzung der eingebetteten Systeme untereinander und mit einem Gateway eingesetzt. Insbesondere spielen dabei verteilte Sensoren eine Rolle.

MORE hatte zum Ziel, die Funktionalität szenarienspezifischer Dienste möglichst auf unterschiedlichen physikalischen Plattformen zu ermöglichen. Der Mehraufwand einer plattformspezifischen Implementierung lässt sich vermeiden, wenn eine Middleware verwendet wird, um auf die Kommunikationsschnittstellen der Hardware zuzugreifen. Die Middleware abstrahiert also die Zugriffe auf die Hardware und führt dazu eine zusätzliche Schicht ein. Insbesondere bei verteilten Systemen kommen Middleware-Technologien zum Einsatz [29].

Das Projekt MORE wurde von der EU im Kontext des 6. Rahmenprogramms gefördert. Als Referenzanwendungen dienen zum einen die Gesundheitsfürsorge per Datenfernübertragung und zum anderen die Fernüberwachung der Umwelt zwecks Früherkennung von Umweltschäden. Die MORE Middleware berücksichtigt dabei nicht nur die Heterogenität und die Ressourcenbeschränkungen der eingebetteten Systeme (z.B. unterschiedliche Betriebssysteme, Rechenleistung oder Leistungsaufnahme) sondern auch die Unterstützung von Skalierbarkeit, Zuverlässigkeit und Sicherheit. Diese Aspekte werden mittels verschiedener Strategien verwaltet. Beim Design der Middleware wurden keine Annahmen in Bezug auf die Kommunikationsverbindungen getroffen. Daher unterstützt sie unterschiedliche Szenarien, von Personal-Area-Networks (PAN) bis zu Weitverkehrsnetzen (WAN) . Die MORE Middleware nutzt das Design-Paradigma *Service-Oriented-Architecture (SOA)*. Die Gesamtarchitektur ist in Abbildung A.4 dargestellt. Ein MORE Node ist in vier Schichten eingeteilt: Vom *Application Layer* aus greifen die Anwendungen über die MORE API auf die MORE Middleware zu. Diese besteht mindestens aus dem *Core Management Service (CMS)* und kann einen oder mehrere *Enabling Services* beinhalten. Die Services sind mittels des *Publish-Subscribe-Modells* mit-

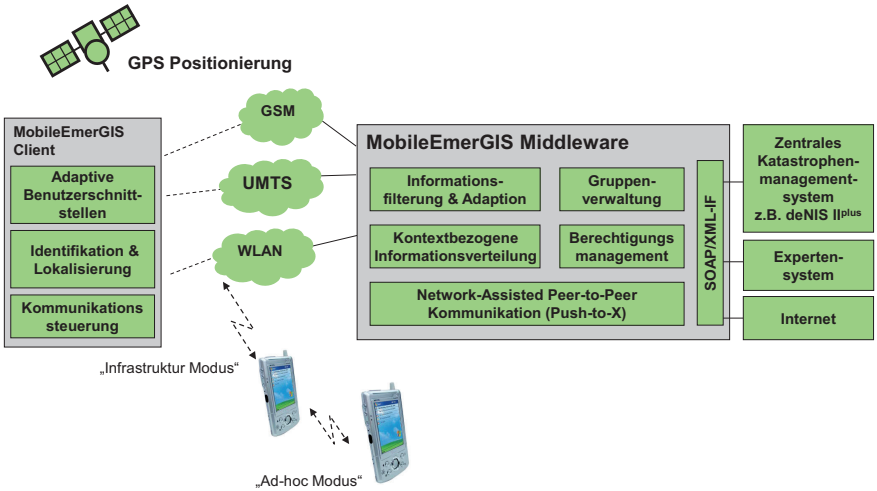


Abbildung A.5: MobileEmerGIS Systemarchitektur [96]

einander verbunden und haben Zugriff auf das Betriebssystem, welches wiederum Zugriff auf die darunterliegende Hardware-Schicht hat.

Von besonderem Interesse für die hier vorliegende Arbeit ist der *µSOA relay service*, welcher die standardisierte Kommunikation mit eingebetteten Systemen ermöglicht, welche nur über geringe Ressourcen verfügen [97]. Dieser Service ist deshalb von Interesse, weil sich der Verfasser der vorliegenden Arbeit im Rahmen von den beiden Projekte Airshield und SPIDER intensiv mit eingebetteten Systemen auseinander gesetzt hat.

A.1.4 MobileEmerGIS

MobileEmerGIS ist ein Projekt in Zusammenarbeit der Dortmunder Feuerwehr, der Firma PRO DV und des Lehrstuhls für Kommunikationsnetze der TU Dortmund. Es soll eine effektivere Kooperation der Einsatzkräfte während eines Großschadenseinsatzes, Katastrophen oder der täglichen Gefahrenabwehr ermöglichen. Ähnlich dem Projekt SPIDER werden dabei die Rettungskräfte der Feuerwehr mittels eines Ad-hoc-Netzes am Einsatzort miteinander vernetzt. Da das Projekt MobileEmerGIS zeitlich vor SPIDER durchgeführt wurde, basiert das Ad-hoc-Netz in MobileEmerGIS auf einer älteren Version der *Dropped Units*.

Die MobileEmerGIS Systemarchitektur ist in Abbildung A.5 dargestellt. MobileEmerGIS Clients sind mittels drahtloser Netze und der MobileEmerGIS Middleware

verbunden. Die Middleware sorgt im Hintergrund unter anderem für die Gruppenverwaltung, die Informationsfilterung und Adaption. Die Middleware basiert dabei auf dem Push-to-X Kommunikationskonzept [75].

Mittels SOAP ist MobileEmerGIS an das zentrale Katastrophenmanagementsystem des Bundes, deNIS II plus, angeschlossen. Weiterhin bietet es die Möglichkeit, ein Expertensystem anzusteuern, oder Inhalte aus dem Internet aufzurufen.

A.2 Weitere Projekte

Nachfolgend werden ein internationales und ein nationales Forschungsprojekt kurz vorgestellt, die ebenfalls die Ad-hoc-Vernetzung von Rettungskräften bei Großschadenslagen zum Thema haben. Dabei wird zunächst das internationale EU-Forschungsprojekt u2010 kurz umrissen, welches das Szenario Brand im Tunnel behandelt. Abschließend wird auf das nationale Forschungsprojekt SoKNOS eingegangen, welches ein Entscheidungs-Unterstützungs-System bereitstellt und dabei die Zusammenarbeit verschiedener Rettungsorganisationen effizienter gestaltet.

A.2.1 u2010

Das Projekt *Ubiquitous IP Centric Government & Enterprise Next Generation Networks, Vision 2010* (u2010) ist ein integriertes Forschungsprojekt des fünften und sechsten Rahmenprogramms der EU, welches von der Universität Luxemburg koordiniert wurde und aus einem Konsortium von 16 Partnern aus 10 europäischen Ländern besteht.

Das übergeordnete Ziel des Projekts ist es, die leistungsfähigsten Kommunikationsmittel und den effektivsten Zugang zu Informationen für jeden, der für die Bekämpfung eines Unfalls, Zwischenfalls, einer Katastrophe oder Krise benötigt wird, wobei existierende und zukünftige Telekommunikationsinfrastrukturen eingesetzt werden.

Das u2010 Projekt untersucht die Fragen der öffentlichen Sicherheit mittels der Erforschung neuer Notfall- und Krisen-Management-Lösungen, auf Basis von innovativen und state-of-the-art Kommunikationstechniken und neuen Internet Technologien (beispielsweise IPv6). Das Anwendungsszenario von u2010 ist ein Brand in einem Tunnel.

Die neuen Technologien, die im Projekt erprobt werden, bieten eine Verbesserung der Verfügbarkeit durch die Zusammenschaltung vorhandener Dienste und Netze im Katastrophenschutz. Damit können redundante Kommunikationswege genutzt

werden, falls die primäre Kommunikation gestört ist. Darüber hinaus können Datenpakete, die im Fehlerfall verloren gegangen sind, automatisch umgeleitet und per Dienstumschaltung fehlerfrei übertragen werden. Ein weiteres Forschungsfeld im Rahmen des Projekts sind drahtlose Ad-hoc-Netze.

A.2.2 SoKNOS

Im nationalen Forschungsprojekt *Service-orientierte ArchiteKturen zur Unterstützung von Netzwerken im Rahmen Öffentlicher Sicherheit* (SoKNOS) werden Konzepte für die Unterstützung staatlicher Organe, Unternehmen und anderer Organisationen, erforscht. Das Ziel von SoKNOS ist die nahtlose Integration von heterogenen Informationsquellen, die den Rettungsorganisationen untereinander eine effiziente Zusammenarbeit erlaubt [19]. Dadurch das SAP bei diesem Projekt Konsortialführer ist, hat es große Aufmerksamkeit erregt.

SoKNOS unterstützt Entscheidungsträger bei folgenden Prozessen. Informationen von verschiedenen und verteilten Umgebungen können schnell gefunden und verfügbar gemacht werden, wobei diese Informationen auch für andere Rettungsorganisationen verfügbar sind. Die Lage wird visuell, allein oder in Zusammenarbeit mit anderen Entscheidungsträgern, aufbereitet, wobei unterschiedliche Entscheidungsunterstützungsalgorithmen eingesetzt werden, die eine Bewältigung der Lage auf einer konsistenten Informationsbasis erlaubt. Neue Informationen können auf eine einfache Art und Weise erstellt werden. Dazu zählen beispielsweise Befehle oder Aufforderungen, aber auch neue geo-referenzierte Objekte, Pläne und Lageinformationen. Darüber hinaus wird auch die Zusammenarbeit mehrerer Einheiten unterstützt. Ferner unterstützt SoKNOS die Entscheidungsträger bei der Integration und Aggregation, sowie der Erstellung von Informationen durch eine stark verbesserte Bedienbarkeit des Systems.

B

Wissenschaftlicher Tätigkeitsnachweis

B.1 Eigene Publikationen

[B.1] Wolff, A.; M. Sbeiti; Wietfeld, C.: *Performance Evaluation of process-oriented wireless relay deployment in Emergency Scenarios*, 17th IEEE Symposium on Computers and Communications (ISCC 2012), Cappadocia, Turkey, Jul 2012.

[B.2] Wolff, A.; Wietfeld, C.: *Process-Oriented Deployment of Ad-hoc Networks in Emergency Scenarios*, IEEE International Conference on Pervasive Computing and Communication (PerCOM 2012), Lugano, Switzerland, Mar 2012.

[B.3] Wolff, A.; Wietfeld, C.: *Performance analysis of 802.11 DCF parameters which support QoS in Emergency Scenarios*, IEEE International Symposium on Wireless Communication Systems (ISWCS 2011), Aachen, Germany, Nov 2011.

[B.4] Pojda J., Wolff A., Sbeiti M., Wietfeld C.: *Performance Analysis of Mesh Routing Protocols for UAV Swarming Applications*, IEEE International Symposium on Wireless Communication Systems (ISWCS 2011), Aachen, Germany, Nov 2011.

[B.5] Sbeiti M., Tran T., Subik S., Wolff A., C. Wietfeld. *MuSE: Novel Efficient Multi-Tier Communication Security Model for Emergency and Rescue Operations*, IEEE MASS Workshop on Mobile Ad-Hoc Networks for Public Safety Systems - WMAPS, Valencia, Spain, Oct 2011.

[B.6] Sbeiti M., Wolff A., Wietfeld C.: *PASER: Position Aware Secure and Efficient Route Discovery for Wireless Mesh Networks*, The Fifth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Nice/Saint Laurent du Var, France, Aug 2011.

[B.7] Daniel, K., Wolff, A. and Wietfeld, C.: *Protocol Design and Delay Analysis for a MUAV-Based Aerial Sensor Swarm*, IEEE Wireless Communications and Networking Conference (WCNC), Sydney, Australia, 2010.

[B.8] Müller, C., Subik, S., Wolff, A. and Wietfeld, C.: *A System Design Framework for Scalability Analysis of Geographic Routing Algorithms in Large-Scale Mesh Networks*, 3rd International OMNeT++ Workshop on the ACM/ICST SIMUTools Conference, Malaga, Spain, ACM/ICST, 2010.

[B.9] Wolff, A., Rohde, S., Subik, S. and Wietfeld, C.: *Organisationsuebergreifender sicherer Datenaustausch zwischen heterogenen Kriseninformationssystemen*, Tagungsband zum Workshop zur IT-Unterstuetzung von Rettungskraeften, 39. Jahrestagung der Gesellschaft fuer Informatik (Informatik 2009), Luebeck, Oct 2009.

[B.10] Seger, J., Lewandowski, A., Wolff, A. and Wietfeld, C.: *Impact of Multilevel Hierarchies on Performance of Wireless Peer-to-Peer Group Communication*, The 70th IEEE Vehicular Technology Conference (VTC), Anchorage, Alaska, IEEE, Sept 2009.

[B.11] Subik, S., Wolff, A. and Wietfeld, C.: *Emergency Digital Telecommunication Standardisation*, Safety & Security International, Mönch Publishing Group, ISSN 1865-9780, pages: 22-24, Dec 2008.

[B.12] Wietfeld, C., Wolff, A. and Subik, S.: *Design and Performance Evaluation of a Wireless Ad-Hoc Emergency Response Management System*, ComNets - Sonderband zur Eröffnung des ComNets-Gebäudes, Wissenschaftsverlag Mainz, ISBN: 3-86130-937-8, pages: 214-225, Nov 2008.

[B.13] Schmutzler, J., Wolff, A. and Wietfeld, C.: *Comparative Performance Evaluation of Web Services and JXTA for Embedded Environmental Monitoring Systems*, 12th International IEEE EDOC Conference, Middleware for Web Services Workshop, Munich, Germany, IEEE, pages: 369-376, Sept 2008.

[B.14] Wolff, A., Subik, S. and Wietfeld, C., *Performance analysis of highly available ad hoc Surveillance Networks Based on Dropped Units*, The 2008 IEEE Technologies for Homeland Security Conference, Boston, MA, USA, IEEE, Vol. 1, pages: 123-128, May 2008.

[B.15] Wolff, A.; Michaelis, S.; Schmutzler, J.; Wietfeld, C.: *Network-centric Middleware for Service Oriented Architectures across Heterogeneous Embedded Systems*, 11th International IEEE EDOC Conference, Middleware for Web Services Workshop, Annapolis, Maryland, USA, 2007.

[B.16] Wietfeld, C. and Wolff, A.: *MobileEmerGIS: a wireless-enabled technology platform to efficiently support field forces in protecting critical infrastructure*, The 2007 IEEE Conference on Technologies for Homeland Security, Woburn, MA, USA, IEEE, Vol. 1, pages: 51 - 56, May 2007.

[B.17] Seger, J.; Wolff, A.; Wietfeld, C., *Analysis of IP-based Real-time Multimedia Group Communication in heterogenous wireless Networks*, The 3rd International Symposium on Wireless Communication Systems (ISWCS 2006), Valencia, Spain, 2006.

B.2 Patentbeteiligungen

[B.18] Beteiligt an: *Access method and communication system for accessing a protected communication service*, Patent angemeldet

[B.19] Beteiligt an: *Integrated-Communication-Hose-System for Firebrigades*, Patent angemeldet

B.3 Betreute Studien- und Diplomarbeiten

[B.20] Bettaieb, M. A.: *Leistungsbewertung von koexistierenden WLAN Netzen mit Prioritäts- und Zuverlässigkeitsanforderungen*, Diplomarbeit TU Dortmund, 2010

[B.21] Chaouech, S.: *Simulative Leistungsbewertung von Relay-basierten multichannel WLAN Systemen*, Diplomarbeit TU Dortmund, 2010

[B.22] Bettaieb, M. A. und Chaouech, S.: *3D-Modellierung für Multiskalen Simulationsumgebungen*, Studienarbeit TU Dortmund, 2008

[B.23] Budde, A.: *Optimierte Distribution von visuellen Lageinformationen für mobile eingebettete Systeme im Katastrophenschutz*, Diplomarbeit TU Dortmund, 2007

[B.24] Subik, S.: *Entwicklung einer multi-skalaren Simulationsumgebung zur Leistungsbewertung von Gruppenkommunikation im Katastrophenschutz*, Diplomarbeit TU Dortmund, 2007

[B.25] Pinschke, S.: *Implementierung und Bewertung einer gruppensynchronisierten Lagebildverteilung für mobile GIS-Clients*, Diplomarbeit TU Dortmund, 2007

[B.26] Subik, S.: *Verschlüsselung von IP-basierter Multimediakommunikation* , Studienarbeit TU Dortmund, 2007

B.4 Durchführung von Lehrveranstaltungen und Lehrkompetenz

[B.27] Seminar: *State-of-the-art system design using formal modelling languages*, TU Dortmund, 2006 (8 Teilnehmer)

[B.28] Übungsgruppenleiter: *Grundlagen der Elektrotechnik*, TU Dortmund, WS 2006/2007

[B.29] Übungsgruppenleiter: *Grundlagen der Elektrotechnik*, TU Dortmund, WS 2007/2008

[B.30] Übungsgruppenleiter: *Mobilfunknetze und ihre Protokolle I*, TU Dortmund, SS 2008

[B.31] Einzelne Übung: *Mobilfunknetze und ihre Protokolle II*, TU Dortmund, SS 2008

[B.32] Übungsgruppenleiter: *Grundlagen der Elektrotechnik*, TU Dortmund, WS 2008/2009

[B.33] Praktikumsleiter: *Betriebswirtschaftliche Grundlagen der Informations- und Kommunikationstechnik*, TU Dortmund, SS 2009

[B.34] Praktikumsbetreuung: *Betriebswirtschaftliche Grundlagen der Informations- und Kommunikationstechnik*, TU Dortmund, SS 2010

Literaturverzeichnis

[1] Ausschuss für Feuerwehrangelegenheiten (AFW), "Feuerwehr-Dienstvorschrift 100 - Führung und Leitung im Einsatz," *http://goo.gl/MeLGz*, vol. 1-54, 1999.

[2] Ausschuss für Feuerwehrangelegenheiten (AFW), "Feuerwehr-Dienstvorschrift 1 - Grundtätigkeiten: Lösch und Hilfleistungseinsatz," *http://goo.gl/hQ5Wy*, pp. 1–166, 2006.

[3] L. Barolli, M. Ikeda, G. D. Marco, A. Durresi, and F. Xhafa, "Performance Analysis of OLSR and BATMAN Protocols Considering Link Quality Parameter," in *2009 International Conference on Advanced Information Networking and Applications*. IEEE, 2009, pp. 307–314.

[4] M. A. Bettaieb, "Leistungsbewertung von koexistierenden WLAN Netzen mit Prioritäts- und Zuverlässigkeitsanforderungen," in *Diplomarbeit TU Dortmund*, 2010.

[5] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535 – 547, 2000.

[6] G. Bianchi, "Email-Antwort von Giuseppe Bianchi <giuseppe.bianchi@uniroma2.it> an Andreas Wolff <andreas.wolff@tu-dortmund.de>. Betreff: Your well known performance analysis of 802.11 WLAN networks." http://goo.gl/40d0e [Online, aufgerufen Juni 2013], 2010.

[7] M. Bowman, "Advanced Mobile Communications for Emergency Management and Crisis Response," in *Proceedings of The 2008 IAJC-IJME International Conference*, Nashville, TN, USA, 2008, pp. 1–10.

[8] R. Bruno, M. Conti, and E. Gregori, "Mesh networks: commodity multihop ad hoc networks," *IEEE Communications Magazine*, vol. 43, no. 3, pp. 123–131, Mar. 2005.

[9] Bundesministerium des Innern, "Beschluss der Innenministerkonferenz vom 23./24. November 2000 zur Einführung eines digitalen Sprech- und Datenfunksystems." per Mail angefragt bei presse@bmi.bund.de am 10.07.2012.

[10] R. C. Carrano, L. C. S. Magalhaes, D. C. M. Saade, and C. V. N. Albuquerque, "IEEE 802.11s Multihop MAC: A Tutorial," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 1, pp. 52–67, 2011.

[11] H. Chang, J. Gao, and P. Pan, "Experiment and Research of Google SketchUp Combine with ArcGIS in the Three-Dimensional Urban Geographic Information System," in *2009 WRI World Congress on Software Engineering*. IEEE, 2009, pp. 309–312.

[12] T. Clausen and P. Jacquet, “Optimized Link State Routing Protocol (OLSR),” in *RFC 3626*, ser. Request for Comments, vol. 54, no. 3626, Internet Engineering Task Force. IETF, http://www.ietf.org/rfc/rfc3626.txt, 2003, pp. 1–76.

[13] R. Colburn, “Milestones: Two-Way Police Radio Communication, 1933,” in *IEEE Global History Network*. http://goo.gl/jje8K [Online, aufgerufen Juni 2013].

[14] D-Link Cooperation, “Product External Specifications for 11n Draft2.0 Dualband USB Dongle - Model Number: DWA-160 A2,” p. 11, 2008.

[15] K. Daniel, A. Wolff, and C. Wietfeld, “Protocol Design and Delay Analysis for a MUAV-Based Aerial Sensor Swarm,” in *2010 IEEE Wireless Communication and Networking Conference*. IEEE, Apr. 2010, pp. 1–6.

[16] J. Deissner, J. Hübner, and D. Hunold, “RPS Radiowave Propagation Simulator: User manual,” in *Radioplan GmbH*. http://goo.gl/dkk6C [Online, aufgerufen Juni 2013].

[17] L. Delosieres and S. Nadjm-Tehrani, “BATMAN store-and-forward: The best of the two worlds,” in *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*. IEEE, Mar. 2012, pp. 721–727.

[18] DIN, “Feuerlöschschläuche - Druckschläuche und Einbände für Pumpen und Feuerwehrfahrzeuge,” *DIN 14811 (2008-01-00)*, p. 10, 2008.

[19] S. Döweling and F. Probst, “Soknos - An Interactive Visual Emergency Management Framework,” in *GeoSpatial Visual Analytics*. Springer, 2009, pp. 251–262.

[20] ETSI, “Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI),” in *European Standard (Telecommunications series) ETSI EN 300 392-2 V2.3.2*, vol. 3, no. V2.3.2. European Telecommunications Standards Institute 2001.

[21] Financial Times Deutschland, “Mobilfunk-Auktion bringt dem Staat nur 4,4 Mrd. Euro,” http://goo.gl/Xd0Se [Online, aufgerufen Juni 2013].

[22] A. G. Fragkiadakis, I. G. Askoxylakis, E. Z. Tragos, and C. V. Verikoukis, “Ubiquitous robust communications for emergency response using multi-operator heterogeneous networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 1, p. 13, 2011.

[23] R. L. Freeman, *Radio System Design for Telecommunication*, third edit ed. John Wiley & Sons, 2006.

[24] F. Gebali, *Analysis of Computer and Communication Networks*. Springer Science + Business Media, 2008.

[25] H.-O. Geisel, “Entwicklung des BOS-Sprechfunks - Grundlagen, Organisation und Technik,” in *Brandschutz - Deutsche Feuerwehr-Zeitung, 7/1999*. Online: http://goo.gl/wA3El [Online, aufgerufen Juni 2013], 1999, pp. 604–616.

[26] M. Geselowitz, “Possible History Milestones in Australia,” in *IEEE Global History Network*. http://goo.gl/oCt24 [Online, aufgerufen Juni 2013].

[27] Gumstix, “Overo Earth COM,” https://www.gumstix.com [Online, aufgerufen Juni 2013].

[28] T. Hadhrami, Q. Wang, M. Crowe, and C. Grecos, “UrgentMesh: Wireless mesh networks with DVB-Satellite for emergency management,” in *2011 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. Budapest: IEEE, 2011, pp. 1–6.

[29] U. Hammerschall, *Verteilte Systeme und Anwendungen*. Pearson Studium, 2005.

[30] G. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke, “IEEE 802.11s: The WLAN Mesh Standard,” *IEEE Wireless Communications Magazine*, vol. 17, no. 1, pp. 104–111, Feb. 2010.

[31] P. Hofmann, K. Kuladinithi, A. Timm-Giel, C. Goerg, C. Bettstetter, F. Capman, and C. Toulsaly, “Are IEEE 802 Wireless Technologies Suited for Fire Fighters?” in *Wireless Conference 2006 - Enabling Technologies for Wireless Multimedia Communications (European Wireless), 12th European*, Munich, Germany, 2006, pp. 1–5.

[32] R. Hornig and A. Varga, “An Overview of the OMNeT++ Simulation Environment,” in *Proceedings of the First International ICST Conference on Simulation Tools and Techniques for Communications Networks and Systems*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, pp. 1–10.

[33] Y. Huang, Y. Gao, and K. Nahrstedt, “Relay Placement for Reliable Base Station Connectivity in Polymorphous Networks,” in *Sensor Mesh and Ad Hoc Communications and Networks (SECON), 2010 7th Annual IEEE Communications Society Conference on*. IEEE, 2010, pp. 1–9.

[34] Y. Huang, S. Bhatti, and D. Parker, “Tuning OLSR,” in *2006 IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE, Sep. 2006, pp. 1–5.

[35] IABG, “HiMoNN - Highly Mobile Network Node,” http://himonn.iabg.de/index.php [Online, aufgerufen Juni 2013].

[36] IEEE, “IEEE Standard for Information Technology Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks Common Specifications Part 3: Media Access Control (MAC).” *IEEE 802.1D*, 1998.

[37] IEEE, “IEEE Std 802.11e-2005,” *(Amendment to IEEE Std 802.11, 1999 Edition)*, 2005.

[38] IEEE, “802.16e-2005 Air Interface for Fixed and Mobile Broadband Wireless Access Systems,” *IEEE Standard for Local and Metropolitan Area Networks Part 16*, 2006.

[39] IEEE, “IEEE Standard for Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs),” *IEEE Std 802.15.4-2011*, 2011.

[40] IEEE, “P802.11s/D12.0, May 2011 IEEE Draft Standard for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical L,” *IEEE 802.11s*, pp. 1–391, 2011.

[41] IEEE, “IEEE Standard for Information technology,” *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pp. 1–2793, 2012.

[42] Iperf Team, “Iperf: The TCP/UDP bandwidth measurement tool,” http://sourceforge.net/projects/iperf/ [Online, aufgerufen Juni 2013].

[43] IRF Dortmund, “Anchors - Das Projekt im Überblick,” http://goo.gl/H9m9F [Online, aufgerufen Juni 2013].

[44] ITU, “Frequency allocations - Kapitel 5.150: Industrial, scientific and medical (ISM) applications,” in *Radio Regulations - Volume 1.* 2004, http://goo.gl/LzX0A , pp. 1-424, [Online, aufgerufen Juni 2013].

[45] D. Johnson, N. Ntlatlapa, and C. Aichele, “Simple pragmatic approach to mesh routing using BATMAN,” in *2nd IFIP International Symposium on Wireless Communications and Information Technology in Developing Countries*, Pretoria, South Africa, 2008, pp. 1–10.

[46] J. Kruskal, “On the shortest spanning subtree and the traveling salesman problem,” in *Proceedings of the American Mathematical Society*, 1956, pp. 48–50.

[47] Y.-W. Kuo and W.-F. Lu, “Delayed Contention DCF MAC Protocol for IEEE 802.11 Wireless LANs,” in *2012 IEEE 75th Vehicular Technology Conference (VTC Spring).* IEEE, May 2012, pp. 1–5.

[48] M. Laddomada and F. Mesiti, “On the Optimization of the IEEE 802.11 DCF: A Cross-Layer Perspective,” *International Journal of Digital Multimedia Broadcasting*, vol. Volume 201, 2010.

[49] A. Lewandowski, R. Burda, S. Subik, and C. Wietfeld, “A Multiscale Simulation Environment for Performance Evaluation of high reliable heterogeneous Communication Networks,” in *European Simulation and Modelling Conference (ESM), Le Havre, France*, 2008, pp. 131–136.

[50] G. Lin, “Steiner tree problem with minimum number of Steiner points and bounded edge-length,” *Information Processing Letters*, vol. 69, no. 2, pp. 53–57, 1999.

[51] H. Liu, J. Li, Z. Xie, S. Lin, K. Whitehouse, J. a. Stankovic, and D. Siu, “Automatic and robust breadcrumb system deployment for indoor firefighter applications,” in *Proceedings of the 8th international conference on Mobile systems, applications, and services - MobiSys ’10*. New York, New York, USA: ACM Press, 2010, p. 21.

[52] MathWorks, “Matlab online documentation - Optimization toolbox: fsolve,” http://www.mathworks.de/de/help/optim/ug/fsolve.html [Online, aufgerufen Juni 2013].

[53] Metageek, “Wi-Spy 2.4x Spectrum Analyser,” http://goo.gl/RGsyM [Online, aufgerufen Juni 2013].

[54] S. Michaelis, A. Lewandowski, K. Daniel, F. Z. Yousaf, and C. Wietfeld, “A comprehensive mobility management solution for handling peak load in cellular network scenarios,” in *Proceedings of the 6th ACM international symposium on Mobility management and wireless access - MobiWac ’08*. New York, New York, USA: ACM Press, Oct. 2008, p. 9.

[55] B. Milic and M. Malek, “Analyzing Large Scale Real-World Wireless Multihop Network,” *IEEE Communications Letters*, vol. 11, no. 7, pp. 580–582, Jul. 2007.

[56] S. Misra, S. D. Hong, G. Xue, and J. Tang, “Constrained Relay Node Placement in Wireless Sensor Networks to Meet Connectivity and Survivability Requirements,” *IEEE INFOCOM The 27th Conference on Computer Communications (2008)*, no. 1, pp. 281–285, 2008.

[57] MSA Auer GmbH, “Leitstellen: Technik folgt Taktik,” in *http://www.git-sicherheit.de/topstories/brandschutz/leitstellen-technik-folgt-taktik*, [Online, aufgerufen Juni 2013], 2010.

[58] D. Naudts, S. Bouckaert, J. Bergs, A. Schoutteet, C. Blondia, I. Moerman, and P. Demeester, “A Wireless Mesh Monitoring and Planning Tool for Emergency Services,” in *2007 Workshop on End-to-End Monitoring Techniques and Services*. IEEE, May 2007, pp. 1–6.

[59] P. C. Ng and S. C. Liew, "Throughput Analysis of IEEE802.11 Multi-Hop Ad Hoc Networks," *IEEE/ACM Transactions on Networking*, vol. 15, no. 2, pp. 309–322, Apr. 2007.

[60] B. Niehoefer, S. Lehnhausen, and C. Wietfeld, "Optimizing Strategies for a Time-Efficient Evaluation of Position-Specific Communication Aspects in Disaster Relief Scenarios," in *IEEE European Space Telecommunications*, Rome, Italy, 2012, pp. 1–6.

[61] K. Park, J. Choi, K. Kang, and Y. Hu, "Malicious or selfish? Analysis of carrier sense misbehavior in IEEE 802.11 WLAN," in *Quality of Service in Heterogeneous Networks*. Springer, 2009, pp. 351–362.

[62] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*. IEEE, 1999, pp. 90–100.

[63] C. Perkins and E. Baccelli, "Multi-hop Ad Hoc Wireless Communication," *IETF Network Working Group - Internet-Draft, http://tools.ietf.org/html/draft-baccelli-manet-multihop-communication-01 [Online, aufgerufen Juni 2013]*, p. 10, 2012.

[64] M. H. Pinson, S. Wolf, and R. B. Stafford, "Video Performance Requirements for Tactical Video Applications," in *2007 IEEE Conference on Technologies for Homeland Security*. IEEE, May 2007, pp. 85–90.

[65] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance analysis of mesh routing protocols for UAV swarming applications," in *2011 8th International Symposium on Wireless Communication Systems*. IEEE, Nov. 2011, pp. 317–321.

[66] Polizeipräsidium Essen, "Vorläufiger Abschlussbericht zur Nachbereitung des polizeilichen Einsatzes der Veranstaltung Loveparade," 2010, http://goo.gl/5LmvS , p. 30, [Online, aufgerufen Juni 2013].

[67] M. Portmann and A. A. Pirzada, "Wireless Mesh Networks for Public Safety and Crisis Management Applications," *IEEE Internet Computing*, vol. 12, no. 1, pp. 18–25, Jan. 2008.

[68] R. Prim, "Shortest connection networks and some generalisations," in *Bell System Technical Journal, 36*, 1957, pp. 1389–1401.

[69] J. Rech, *Wireless LANs: 802.11-WLAN-Technologie und praktische Umsetzung im Detail*. Heise, 2006.

[70] S. Rohde, N. Goddemeier, C. Wietfeld, F. Steinicke, K. Hinrichs, T. Ostermann, J. Holsten, and D. Moormann, "AVIGLE: A system of systems concept for an avionic digital service platform based on Micro

Unmanned Aerial Vehicles," in *2010 IEEE International Conference on Systems, Man and Cybernetics*. IEEE, Oct. 2010, pp. 459–466.

[71] M. Sbeiti, J. Pojda, and C. Wietfeld, "Performance evaluation of PASER - An efficient secure route discovery approach for wireless mesh networks," in *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*. IEEE, Sep. 2012, pp. 745–751.

[72] M. Sbeiti, A. Wolff, and C. Wietfeld, "PASER: Position Aware Secure and Efficient Route Discovery for Wireless Mesh Networks," in *The Fifth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE)*, Nice/Saint Laurent du Var, France, 2011, pp. 63–70.

[73] C. Schilling, N. Langhammer, B. Aznar, and R. Kays, "HOMEPLANE: An architecture for a wireless home area network with management support for high quality of service," in *2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE, Sep. 2008, pp. 1–5.

[74] L. Schori, "Mesh Netzwerke mit OLSR und B.A.T.M.A.N," in *Open Students Lunch Zürich*. Online am 08.11.12: http://goo.gl/8wkZ4, 2009.

[75] D. Schraven, "Loveparade-Planungsfehler bei Polizei massiver als bekannt," in *WAZ vom 09.02.2012*, http://goo.gl/Rft9j [Online, aufgerufen Juni 2013].

[76] J. Seger, *Gruppenkommunikationssystem für mobile Multimediaanwendungen mit Echtzeitanforderungen Entwurf, Implementierung und Leistungsbewertung*. Dissertation TU Dortmund, 2008.

[77] F. Senf, "ITCS im Ruhrgebiet: Status Quo des RBL-KöR," in *Beka Seminar*. http://www.itcs-info.de/download/ITCS_Treffpunkt_Okt_09/Senf.pdf [Online, aufgerufen Juni 2013], 2009.

[78] Small Cell Forum, "Small cells - what's the big idea?" http://smallcellforum.org/smallcellforum/resources-white-papers, p. 17. [Online, aufgerufen Juni 2013].

[79] D. R. Smith, *Digital Transmission Systems*. Springer, 2004.

[80] M. R. Souryal, A. Wapf, and N. Moayeri, "Rapidly-Deployable Mesh Network Testbed," *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, pp. 1–6, Nov. 2009.

[81] Spiegel, "Unser Feuer machen wir selber aus," in *Der Spiegel 34/1975*. http://www.spiegel.de/spiegel/print/d-41458053.html [Online, aufgerufen Juni 2013], 1975, pp. 17–26.

[82] F. Spitzer, *Principles of random walk*. Springer-Verlag, 2001.

[83] W. Stallings, *Wireless communications and networks*, second edi ed. Pearson Prentice Hall, 2005.

[84] J. C. Stein, "Indoor Radio WLAN Performance - Part II: Range Performance in a Dense Office Environment," in *White Paper*, 1998, pp. 1–9.

[85] T. Stoeveken, "MJPG-streamer release 94," in *http://sourceforge.net/projects/mjpg-streamer/*, [Online, aufgerufen Juni 2013].

[86] S. Subik, S. Rohde, T. Weber, and C. Wietfeld, "SPIDER: Enabling interoperable information sharing between public institutions for efficient disaster recovery and response," in *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*. IEEE, 2010, pp. 190–196.

[87] S. Subik, "Verschlüsselung von IP-basierter Multimediakommunikation," in *Studienarbeit TU-Dortmund*, 2007.

[88] S. Szott, M. Natkaniec, R. Canonico, and A. Pach, "Misbehaviour Analysis of 802.11 Mobile Ad-Hoc Networks - Contention Window Cheating," in *Med Hoc Net*, 2007, pp. 12–15.

[89] A. Timm-Giel, K. Kuladinithi, P. Hofmann, and C. Görg, "Wireless and Ad Hoc Communications Supporting the Firefighter," in *15th IST Mobile and Wireless Summit*, Mykonos, Greece, 2006, pp. [DVD p. 1–5].

[90] P. Tran-Gia, *Einführung in die Leistungsbewertung und Vehrkehrstheorie*, 2nd ed. pp. 153-154: Oldenbourg Wissenschaftsverlag GmbH, 2005.

[91] A. Vahdat and D. Becker, "Epidemic Routing for Partially-Connected Ad Hoc Networks," in *Duke Tech Report CS-2000-06*. Durham, North Carolina: Duke University, 2000, p. 10.

[92] A. Varga, "The OMNeT++ discrete event simulation system," in *Proceedings of the European Simulation Multiconference (ESM 2001)*, vol. 9, 2001.

[93] B. Walke, *Mobilfunknetze und ihre Protokolle 1, Grundlagen, GSM, UMTS und andere zellulare Mobilfunknetze*. Vieweg+Teubner Verlag; Auflage: 3., überarb. u. akt. Aufl. 2001, 2001.

[94] B. H. Walke, S. Mangold, and L. Berlemann, *IEEE 802 Wireless Systems: Protocols, Multi-Hop Mesh/Relaying, Performance and Spectrum Coexistence*. Wiley, 2006.

[95] C. Wietfeld, "Krisenkommunikation und Technik," in *Forschungsforum Öffentliche Sicherheit*. Freie Universität Berlin, http://goo.gl/yGQLB [Online, aufgerufen Juni 2013].

[96] C. Wietfeld, "Klassifizierung von Mobilfunknetzen," in *Vorlesungsunterlagen Mobilfunknetze und Protokolle*. TU Dortmund, 2013.

[97] C. Wietfeld, A. Wolff, and U. Bieker, "MobileEmerGIS: a Wireless-enabled Technology Platform To Support Emergency Response Management," in *2007 IEEE Conference on Technologies for Homeland Security*. Boston, MA: IEEE, 2007, pp. 51–56.

[98] A. Wolff, S. Michaelis, J. Schmutzler, and C. Wietfeld, "Network-centric Middleware for Service Oriented Architectures across Heterogeneous Embedded Systems," in *2007 Eleventh International IEEE EDOC Conference Workshop*, no. October. IEEE, Oct. 2007, pp. 105–108.

[99] A. Wolff, S. Rohde, S. Subik, and C. Wietfeld, "Organisationsübergreifender sicherer Datenaustausch zwischen heterogenen Kriseninformationssystemen," in *JENAER SCHRIFTEN*, 2009, pp. 1–5.

[100] A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance evaluation of process-oriented wireless relay deployment in emergency scenarios," in *2012 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, Jul. 2012, pp. 651–654.

[101] A. Wolff, S. Subik, and C. Wietfeld, "Performance Analysis of Highly Available Ad Hoc Surveillance Networks Based on Dropped Units," in *2008 IEEE Conference on Technologies for Homeland Security*. IEEE, 2008, pp. 123–128.

[102] A. Wolff and C. Wietfeld, "Performance analysis of 802.11 DCF parameters which support QoS in emergency scenarios," in *2011 8th International Symposium on Wireless Communication Systems*. IEEE, Nov. 2011, pp. 629–633.

[103] A. Wolff and C. Wietfeld, "Process-oriented deployment of ad-hoc networks in emergency scenarios," in *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*. IEEE, Mar. 2012, pp. 728–733.

[104] L. Xiong and G. Mao, "Saturated throughput analysis of IEEE 802.11 e EDCA," *Computer Networks*, vol. 51, no. 11, pp. 3047–3068, 2007.

[105] L. Xiong, "A Markov Chain Approach to IEEE 802.11 WLAN Performance Analysis," Ph.D. dissertation, University of Sydney, 2008.

[106] A. Yarali, B. Ahsant, and S. Rahman, "Wireless Mesh Networking: A Key Solution for Emergency & Rural Applications," *2009 Second International Conference on Advances in Mesh Networks*, pp. 143–149, Jun. 2009.

[107] J.-Y. Yoo and J. W. Kim, "Maximum End-to-End Throughput of Chain-Topology Wireless Multi-Hop Networks," in *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*, 2007, pp. 11–15.

[108] M. Younis and K. Akkaya, "Strategies and techniques for node placement in wireless sensor networks: A survey," *Ad Hoc Networks*, vol. 6, no. 4, pp. 621–655, 2008.

[109] F. Z. Yousaf, K. Daniel, and C. Wietfeld, "Performance Evaluation of IEEE 802.16 WiMAX Link With Respect to Higher Layer Protocols," in *4th International Symposium on Wireless Communication Systems - ISWCS2007*. IEEE, Oct. 2007, pp. 180–184.

[110] G. Zaggoulos and A. Nix, "WLAN/WDS Performance using Directive Antennas in Highly Mobile Scenarios: Experimental Results," in *2008 International Wireless Communications and Mobile Computing Conference*. IEEE, Aug. 2008, pp. 700–705.

[111] D. Zivadinovic, "Betriebserweiterung - Access-Points zum Aufbau von WLAN-Brücken," http://www.heise.de/mobil/artikel/Konzepte-226065.html [Online, aufgerufen Juni 2013].