



ANCHORS

UAV-Assisted Ad Hoc Networks for Crisis Management and Hostile Environment Sensing

Schlussbericht TU Dortmund



Zuwendungsempfänger Technische Universität Dortmund – Lehrstuhl für Kommunikationsnetze	Förderkennzeichen 13N12204
Vorhabensbezeichnung UAV-Assisted Ad Hoc Networks for Crisis Management and Hostile Environmental Sensing	
Teilvorhabensbezeichnung Schwarmkollaborative Vernetzung heterogener Robotersysteme	
Laufzeit des Vorhabens 01.05.2012 – 31.10.2015	
Teilprojektleiter Prof. Dr.-Ing. Christian Wietfeld Technische Universität Dortmund – Lehrstuhl für Kommunikationsnetze	
Autoren Christian Wietfeld, Daniel Behnke, Sebastian Rohde, Robert Falkenberg, Niklas Goddemeier, Dennis Kaulbars	



Bundesministerium
für Bildung
und Forschung



The ANCHORS – Project is co-financed
by BMBF and ANR



Inhaltsverzeichnis

1. Kurze Darstellung.....	5
1.1 Aufgabenstellung.....	5
1.2 Voraussetzungen für die Durchführung des Vorhabens.....	7
1.3 Planung und Ablauf des Vorhabens.....	7
1.4 Wissenschaftlicher und Technischer Stand.....	9
1.5 Zusammenarbeit mit anderen Stellen.....	11
2. Projektergebnisse.....	13
3. AP 1 - Systemanforderungen und Systemarchitektur.....	13
4. AP 4 – Vehicular Ad-Hoc Communication System.....	15
4.1 Analyse von Kommunikationsnetzen und Verhaltensoptimierung.....	15
4.2 Content-aware Hybrid Communication System Design.....	27
4.3 Mobile Ad-hoc LTE Zellen.....	31
4.4 Ad-hoc Multi-hop Kommunikation.....	44
5. AP 5 – Cooperative Swarm Behavior.....	48
5.1 Architektur der Schwarmsubsysteme.....	48
5.2 Spezifikation der Agenten-basierten Schwarmalgorithmen.....	52
5.3 Multikriterielle Optimierung von Mobilitätsverhalten.....	60
5.4 Dynamisches Rollen-Management.....	66
6. AP 6 – Platform Integration & System Validation.....	70
6.1 Meilenstein 1 – Early Demonstrator.....	70
6.2 Meilenstein 2 – Großübung in Dortmund.....	71
6.3 Meilenstein 3 – Abschluss der Verlängerungsphase.....	72
6.4 Übersicht der Integrationsmeetings.....	73
7. Zahlenmäßiger Nachweis der wichtigsten Positionen.....	74
8. Notwendigkeit und Angemessenheit der geleisteten Arbeit.....	75
9. Voraussichtlicher Nutzen, Verwertbarkeit des Ergebnisses im Sinne des Verwertungsplans.....	76
9.1 Forschung.....	76
9.2 Lehre.....	76
10. Bekanntgewordene Fortschritte Dritter.....	77
11. Erfolge und geplante Veröffentlichungen.....	77

1. Kurze Darstellung

1.1 Aufgabenstellung

Durch den Einsatz und die intelligente Kombination autonomer, unbemannter Systeme ermöglicht das Forschungsprojekt ANCHORS eine schnelle und effektive Fernerkundung sicherheitsrelevanter Ereignisse. Sicherheitsrelevante Ereignisse sind in diesem Kontext technische Großunfälle in Kernkraftwerken oder verteilte Großschadenslagen nach Naturkatastrophen (so genannte „Man-Made-„ und „Natural-Hazards“). Der effiziente Informationsfluss wird dabei unter Berücksichtigung eines Totalausfalles existierender Kommunikationsinfrastrukturen durch eine neuartige, hybride ad-hoc Vernetzung aller beteiligten Entitäten die Handlungsfähigkeit des Krisenmanagements sowie die Sicherheit der Krisenkräfte sicherstellen.

Im Rahmen des Projektes entwickelt das Communication Networks Institute (CNI) der TU Dortmund neuartige Kommunikationssysteme und -verfahren, die einen Informationsaustausch aller in ANCHORS vorgesehenen Entitäten in schwierigen Einsatzumgebungen ermöglichen wird.

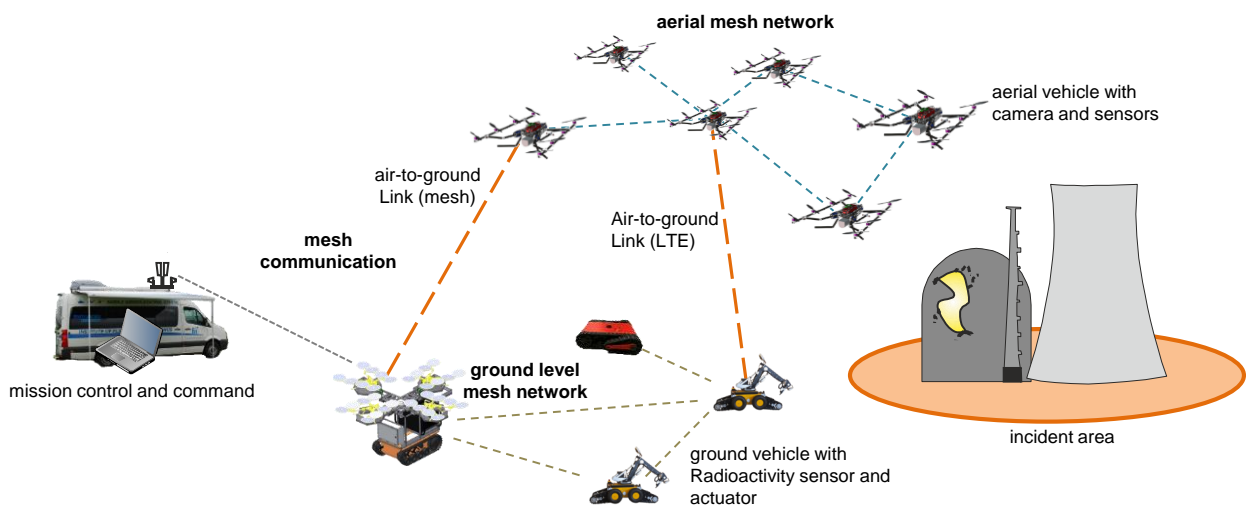


Abbildung 1: Heterogene Ad-Hoc Kommunikation am Einsatzort (Quelle: TU Dortmund)

Ziel I: Protokoll- und Systementwurf zur Bereitstellung von Backend-Services

Das anvisierte ANCHORS-System besteht aus zahlreichen Subsystemen, die einer Vernetzung bedürfen. Die Schnittstellen zwischen den Systemen müssen über logische Protokolle definiert werden, um einen Informationsaustausch und damit die Funktionsfähigkeit des Gesamtsystems zu ermöglichen. Ein grundlegendes Arbeitsziel besteht daher darin, die Subsysteme über geeignete Protokolle zusammenzuführen. Der Protokollentwurf muss dabei die Eigenschaften der genutzten physikalischen Träger berücksichtigen. Das Ziel ist es, an geeigneten Stellen verfügbare Standards einzusetzen und darüber hinaus eine oder mehrere einheitliche Schnittstellen zu

definieren, die als Vorbereitung für eine Standardisierungsaktivität auch über das ANCHORS-spezifische Ziel hinaus eine allgemeine Verwendung ermöglichen.

Ziel II: Vernetzung verteilter Gefahrenlagen über Multi-hop relaying

Neben der Erhebung von Sensordaten ist die Vernetzung der Rettungskräfte vor Ort von strategischer Bedeutung. In Rahmen von ANCHORS werden hierzu neue Protokolle und Konzepte entworfen, die auch bei verteilten Schadenslagen eine Sprach- und Multimedia-Kommunikation ermöglichen. Hierzu werden avionische Funkrelays genutzt, die dynamisch und Punkt-genau platziert eine Krisenkommunikation ermöglichen. Der zentrale Untersuchungsgegenstand besteht dabei darin, mehrere verteilte Schadenslagen miteinander zu vernetzen, indem UAVs als Relay zum Einsatz kommen. Um den Anforderungen der Einsatzkräfte gerecht zu werden, wird hierzu ein System entworfen, welches klassische Dienste aus PMR (Professional Mobile Radio), wie zB. Direct Mode, auch in Netzen der übernächsten Generation, wie LTE Advanced, realisiert. Vor diesem Hintergrund sollen die Realisierbarkeit und Skalierbarkeit dieser Dienste über mehrere UAV-integrierte Relay-Hops im Hinblick auf restriktive Anforderungen an die Latenzzeiten analysiert und bewertet werden.

Ziel III: Kooperative Vernetzung des heterogenen Roboterschwarms

Über die Vernetzung autonomer UGVs (Unmanned Ground Vehicles) untereinander stellt die dynamische und heterogene Vernetzung zwischen UAVs und UGVs ein zentrales Arbeitsziel dar. Aufgrund der Mobilität von UAVs und UGVs sowie der signifikant unterschiedlichen Höhen, die sich wesentlich auf die Funkausbreitung auswirken, unterliegt die heterogene UxV-Vernetzung sehr spezifischen Anforderungen.

Ein Weg diesen Anforderungen zu begegnen ist der Einsatz von ad-hoc Relays. Hierfür wird ein dynamisches Rollenmanagement implementiert um jede Entität dort einzusetzen, wo aktuell der größte Bedarf besteht.

Dabei sind multikriterielle Zielvorgaben zu berücksichtigen. Zum einen ist die effiziente und situations-bedingte Erkundung als Primärziel zu gewährleisten; zum anderen soll kontinuierlich die Kommunikation zwischen den Entitäten (UxVs, Rettungskräfte) möglich sein. Weiterhin sind energetische Aspekte des Health Managements der Roboter zu adressieren.

Untersuchungsgegenstand ist dabei unter anderem die Gewährleistung definierter QoS-Parameter. Hierbei werden Verbindungsabbrüche zwischen den Entitäten berücksichtigt. Je nach Art der zu übertragenen Daten kann eine kontinuierliche Kommunikation nötig sein oder definierte Verbindungsabbrüche akzeptiert werden um beispielsweise größere Strecken durch Data Ferrying überwinden zu können.

1.2 Voraussetzungen für die Durchführung des Vorhabens

Voraussetzung zur Durchführung der praktischen Tests des ANCHORS Systems, basierend auf den verschiedenen Stadien des Prototypen, war eine „Allgemeinerlaubnis zum Aufstieg von unbemannten Luftfahrtsystemen mit einer Gesamtmasse bis zu 5kg“ der Bezirksregierung Münster, die seit August 2012 vorlag und bis zum Ende des Projektes fortlaufend verlängert wurde. Diese Erlaubnis ist jedoch mit einigen für das Projekt relevanten Auflagen und Einschränkungen versehen:

- Die maximale Flughöhe darf 100m über Grund (AGL) nicht übersteigen.
- Der Betrieb über Menschen und Menschenansammlungen ist nicht gestattet.
- Das System muss zu jedem Zeitpunkt von einem geschulten Piloten überwacht werden.

Weiterhin wurde für jeden im Projekt eingesetzten Piloten eine Haftpflichtversicherung abgeschlossen.

Für die Nutzung von Grundstücken für die Flugexperimente lagen jeweils Einverständniserklärungen der Eigentümer zur Grundstücksnutzung vor.

Für die Erprobung der IEEE 802.11s Funktechnologie im Rahmen der Großübung der Dortmunder Feuerwehr am 18.04.2015 war zudem eine Funklizenz der Bundesnetzagentur notwendig.

Durch eine gute interdisziplinäre Zusammenarbeit zwischen Industrie, Wissenschaft mit Einbringung der jeweils besonderen Kompetenzen und die intensive Einbindung der Anwenderseite waren die Voraussetzungen gegeben, das Vorhaben ANCHORS erfolgreich durchzuführen.

1.3 Planung und Ablauf des Vorhabens

Das Vorhaben ANCHORS wurde als Verbundforschungsprojekt mit Mitteln des Bundesministeriums für Bildung und Forschung gefördert und lief 01.05.2012 bis zum 31.10.2015. Der Lehrstuhl für Kommunikationsnetze, in Person von Prof. Dr.-Ing. Christian Wietfeld, übernahm die Rolle der Spokeperson des Deutsch-Französischen Gemeinschaftsprojekts. Zudem leitete der Lehrstuhl das Arbeitspaket 5 – Cooperative Swarm Behavior.

Die Abbildung 2 zeigt die Ressourcenplanung des Projekts.

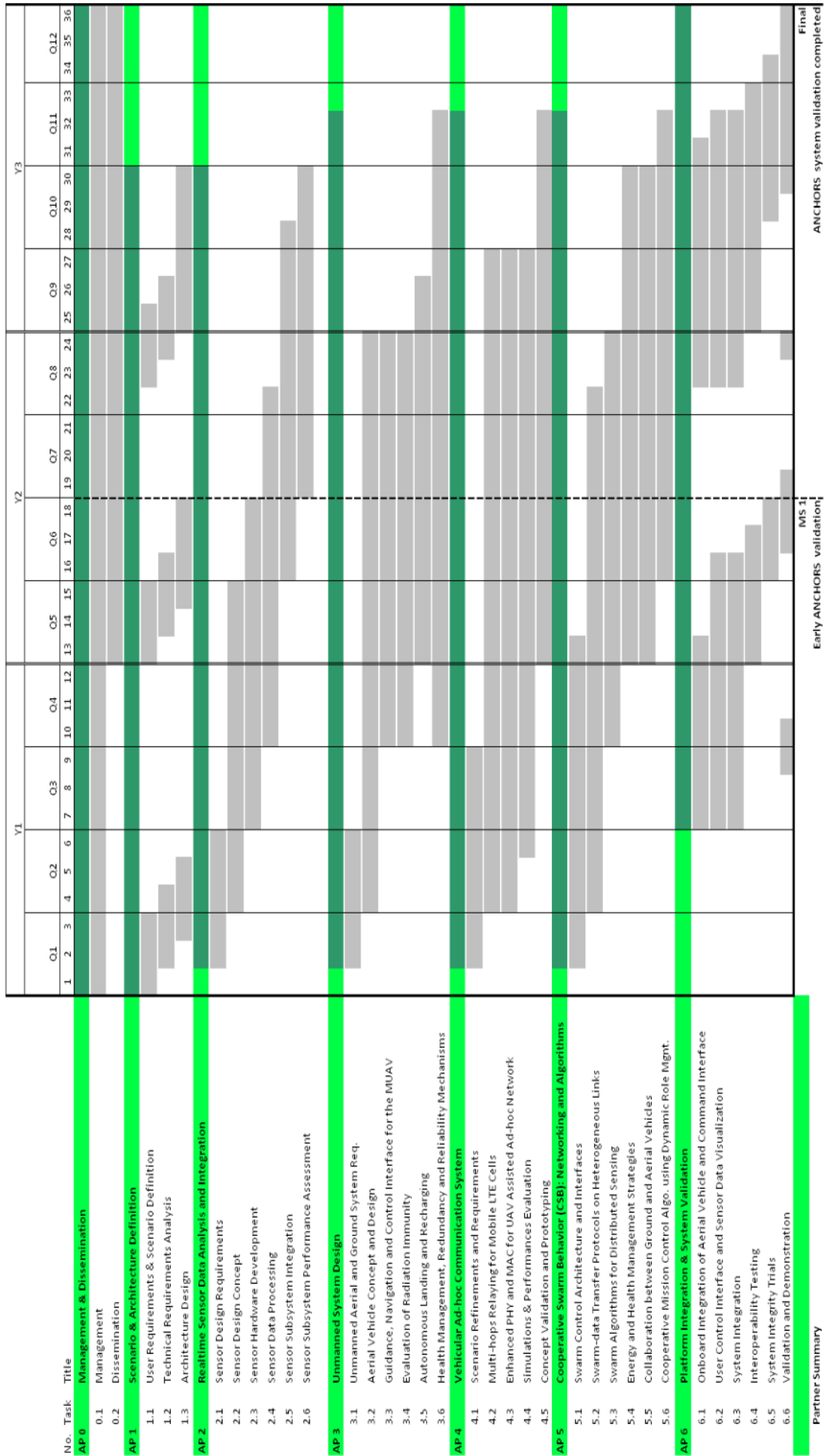


Abbildung 2: Vorhabensbezogene Ressourcenplanung

Der Lehrstuhl für Kommunikationsnetze war an folgenden Arbeitspaketen beteiligt:

- AP 1: Scenario & Architecture Definition
- AP 2: Realtime Sensor Data Analysis and Integration
- AP 4: Vehicular Ad-hoc Communication System
- AP 5: Cooperative Swarm Behavior: Networking and Algorithms
- AP 6: Platform Integration & System Validation

1.4 Wissenschaftlicher und Technischer Stand

Long Term Evolution (LTE)

Der OFDMA-basierte LTE-Standard bietet im Vergleich zu den 3G-Vorgängertechnologien hochdatenratige Kommunikationsverbindungen auf IP-Ebene. Die Verbindungen sind über hohen Datenraten hinaus durch geringe Delays gekennzeichnet. Von besonderer Bedeutung im ANCHORS Kontext sind zudem sogenannte LTE Relays und Femtozellen [1] als neuartige Netzelemente. Hierdurch wird es möglich auch dort LTE Kapazitäten zu schaffen, wo öffentliche Netze nicht oder nicht mehr verfügbar sind.

Aktuell sind diese neuartigen Netzelemente jedoch ausschließlich für den stationären Einsatz ausgelegt. Mobile Femtozellen oder ad-hoc platzierte Relays werden aufgrund der großen Herausforderungen im Bereich der Interferenz-Vermeidung bis jetzt ausschließlich theoretisch und simulativ untersucht [2]. Erste Ansätze diese Konzepte in Richtung einer Versorgung aus der Luft zu erweitern sind noch im Anfangsstadium. Auch die Evaluierung von komplexeren Kapazitätsoptimierungen in LTE Zellen durch Verwendung mehrerer neuartiger Elemente („Multi-Hop“ Relaying) sowie die hiermit verbundenen Auswirkungen auf das Kernnetz sind bis jetzt nur unzureichend untersucht.

- [1] V. Chandrasekhar and J. Andrews, „**Femtocell Networks: A Survey**“, *IEEE Communication Magazine*, Seiten 59- 67, September 2008
- [2] G. Baudreau, J. Panicker, N. Guo, R. Chang, N. Wang and S. Vrzic, „**Interference Coordination and Cancellation for 4G Networks**“, *IEEE Communication Magazine*, Seiten 74 – 80, April 2009

Mesh-Standard - IEEE 802.11s

Der sich zur damaligen Zeit im Standardisierungsprozess befindliche Standard IEEE 802.11s bringt gute Voraussetzungen mit, um auf den UxV Plattformen als Routing Plattform eingesetzt werden zu können. IEEE 802.11s vereinigt im Routingverfahren „Hybrid Wireless Meshing Protocol“ (HWMP) einen reaktiven und proaktiven Teil. Mit dem reaktiven Teil werden Routen nur aufgebaut, wenn sie wirklich gebraucht werden.

Mit dem proaktiven Teil werden Routen nur zu einem bestimmten Wurzelknoten aufgebaut. Die Leistungsvalidierung des Standards und seines Routingprotokolls ist bisher nur in sehr wenigen Publikationen durchgeführt worden [1] [2]. Insbesondere im Hinblick auf Mobilität wurde der 802.11s Standard bisher unzureichend untersucht. Durch das Extensible path selection framework können eigene Routingprotokolle im IEEE 802.11s Standard eingesetzt werden.

- [1] J.-P. Wang, B. Hagelstein, and M. Abolhasan, "**Experimental Evaluation of IEEE 802.11s Path Selection Protocols in a Mesh Testbed**," in *4th International Conference on Signal Processing and Communication Systems (ICSPCS)*, Dec. 2010, pp. 1 –3.
- [2] R. G. Garroppo, S. Giordano, and L. Tavanti, "**Experimental Evaluation of Two Open Source Solutions for Wire-less Mesh Routing at Layer Two**," in *5th IEEE International Symposium on Wireless Pervasive Computing (ISWPC)*, May 2010, pp. 232

Autonome Roboter Systeme und Roboterschwärme

Einzelne verfügbare Systeme weisen bereits einen hohen Grad an Autonomie auf und können für Mess- und Erkundungsaufgaben eingesetzt werden [1].

Kooperierende autonome Roboter sind Gegenstand der Forschung an vielen Institutionen, z.B.: [2] [3], da dieses interdisziplinäre Feld viele hochaktuelle Forschungsfelder vereint. Derzeit existieren Experimentalplattformen mit denen Schwarmverhalten und kooperative Lösungsansätze untersucht werden. Besonders wichtig bei der Kooperation ist stets die Maschine-zu-Maschine Kommunikationsfähigkeit. Aus diesem Grund liegen aktuelle Forschungsschwerpunkte auf Kommunikationsstrategien [4], kommunikationssensitiven Mobilitätsstrategien [6] und der dynamischen Aufgabenverteilung im UAV / UGV Verbund [5], [6]. Die Heterogenität der Netzelemente wurde dabei unter den Gesichtspunkten dynamischer Rollen und kommunikationssensitiven Mobilitätsstrategien bisher nur unzureichend untersucht. Insbesondere unterscheidet sich ANCHORS durch die hohen Anforderungen an die Datenübertragung (Echtzeit PMR und Sensordaten) von bisherigen Forschungsarbeiten.

- [1] AirRobot GmbH [<http://www.airrobot.de>].
- [2] Universität Stuttgart, Institut für Parallele und Verteilte Systeme [<http://www.ipvs.uni-stuttgart.de>]
- [3] ETH Zürich, Autonomous Systems Lab [<http://www.asl.ethz.ch/>]
- [4] Pengcheng Zhan, Kai Yu and Swindlehurst, A.L.; "**Wireless Relay Communications with Unmanned Aerial Vehicles: Performance and Optimization**," *Aerospace and Electronic Systems, IEEE Transactions on*, vol.47, no.3, pp.2068-2085, July 2011
- [5] A. Undurti, J. How. "**A decentralized approach to multi-agent planning in the presence of constraints and uncertainty**," *Robotics and Automation (ICRA), 2011 IEEE International Conference on*, vol., no., pp.2534-2539, 9-13 May 2011
- [6] Phan, C.; Liu, H.H.T.: "**A cooperative UAV/UGV platform for wildfire detection and fighting**," *System Simulation and Scientific Computing, 2008. ICSC 2008. Asia Simulation Conference - 7th International Conference on*, vol., no., pp.494-498, 10-12 Oct. 2008

1.5 Zusammenarbeit mit anderen Stellen

Das Verbundvorhaben wurde von der

- Technischen Universität Dortmund, Lehrstuhl für Kommunikationsnetze (*Kürzel: TUDO*)

mit den folgenden Projektpartnern durchgeführt:

- Ascending Technologies (*ASC*)
- AIRBUS Defense & Space (*AIR*)
- Kerntechnische Hilfsdienst GmbH (*KHG*)
- LS telcom SAS (*LST*)
- Mirion Health Physics (*MIR*)
- SGE GmbH (*SGE*)
- Commissariat à l'énergie atomique et aux énergies alternatives (*CEA*)
- Fraunhofer INT (*INT*)
- RWTH Aachen – Institut für Flugsystemdynamik (*RWTH*)
- ONERA (*ON*)
- Stadt Dortmund, Feuerwehr Dortmund – IFR (*IFR*)
- Groupe-Intra (*GRI*)
- Feuerwehr Frankfurt a.M. (Assoziierter Partner)
- LKA Berlin (Assoziierter Partner)
- Bundesamt für Strahlenschutz (Assoziierter Partner)

Die Projektarbeiten für die im Projektplan vorgesehenen Arbeitspakete wurden in enger Abstimmung mit den jeweils daran beteiligten Projektpartnern durchgeführt. Darüber hinaus fand im Verbundprojekt keine Kooperation mit Dritten statt. Tabelle 1 stellt die Hauptschnittstellen zu jedem der beteiligten Konsortialpartner dar.

Projektpartner	Hauptaufgabe	Schnittstellen zur TU Dortmund
ASC	Flugplattform und Technische Koordination	Hard- und Software-Interface von Flugplattform zu Schwarmsteuerung
AIR	Kommunikationsarchitektur und PMR-Kommunikation	Gemeinsame Definition der Kommunikationsanforderungen und –lösungen
KHG	Szenariodefinition und Validierung	Hard- und Softwareschnittstellen zu Bodenfahrzeugen der KHG

LST	Kommunikationsarchitektur und Missionsplanung	Gemeinsame Definition der Kommunikationsanforderungen und –lösungen
MIR	Entwicklung des RN-Sensors	Softwareschnittstelle zum Sensor
SGE	Entwicklung der Lande- und Ladestation	Lademöglichkeit für Bodenroboter
CEA	Kommunikationsarchitektur und LTE Direct-Mode Betrieb	Gemeinsame Definition der Kommunikationsanforderungen und –lösungen
INT	Untersuchung der Auswirkungen radioaktiver und elektromagnetischer Strahlung auf Gesamtsystem	Test der gewählten Hardware auf Unverträglichkeit
RWTH	Entwicklung des Mobile Mission Control Center (MMCC); automatische Landung	Hard- und Softwareschnittstellen im MMCC sowie auf der Flugplattform
ON	Missionsplanung und Systemvalidierung	Cooperative Swarm Behavior und Planung der Validierungsszenarien
IFR	Szenariodefinition und Validierung	Enge Kooperation bei der Erstellung der Szenarien und Vorbereitung der Demonstrationen
GRI	Szenariodefinition und Validierung	Enge Kooperation bei der Erstellung der Szenarien und Anforderungen

2. Projektergebnisse

Im Folgenden soll die Verwendung der Zuwendung durch die im Projektverlauf erzielten Ergebnisse im Einzelnen dargestellt werden. Die Gliederung der Ergebnisse orientiert sich im Nachfolgenden an die Arbeitspakete mit Verweis auf die im Abschnitt 1.1 beschriebenen Ziele.

Die TU Dortmund ist in ANCHORS insbesondere an den Arbeitspaketen 1, 4, 5 und 6 beteiligt gewesen. Im Folgenden werden die Ergebnisse aus den einzelnen Arbeitspaketen eingehend vorgestellt.

3. AP 1 - Systemanforderungen und Systemarchitektur

Im Arbeitspaket 1 wurden die Szenarien definiert und die Anforderungen an das System spezifiziert. Aus diesen Anforderungen wurde die generelle Systemarchitektur abgeleitet, die die Aufgaben aller Systemkomponenten und ihre Schnittstellen ausweisen soll.

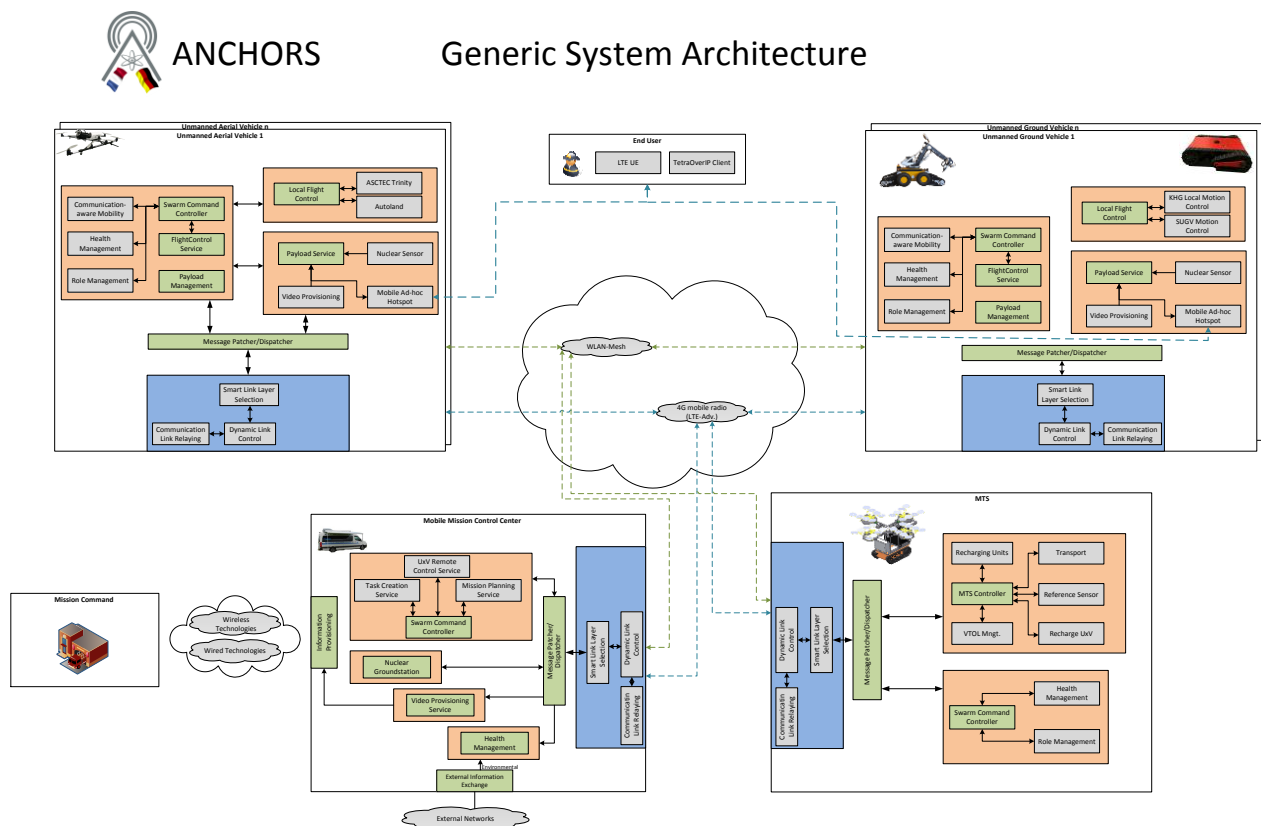


Abbildung 3: Generische System-Architektur (Quelle: TU Dortmund)

Die Abbildung 3 zeigt die generische Systemarchitektur von ANCHORS. Die Systemarchitektur soll alle Komponenten einführen und deren grobe Funktionen darlegen. Detailliertere Einblicke insbesondere zu den Aspekten der Vernetzung und

des kooperativen Schwarmverhaltens finden sich in den Kapiteln 4 und 5. Im Folgenden werden die einzelnen Komponenten eingehender vorgestellt.

Mobile Mission Control Center (MMCC)

Das MMCC ist die Missionszentrale im System. Im diesem Fahrzeug befinden sich die Missionsoperatoren des Roboterschwarms und die Sensoranalysten. Die primären Missionsziele für den Sensorschwarm werden hier festgelegt. Das Fahrzeug wird am Einsatzort, aber nicht in der unmittelbaren Nähe des Unfallorts sein.

Mobile Carrier System (MTS)

Das MTS nimmt im ANCHORS System eine besondere Rolle ein. Mit dem MTS erreichen die kleineren Bodenroboter sowie die Flugroboter das unmittelbare Einsatzgebiet. Die UAVs starten und landen automatisch vom MTS und die Batterien werden wieder aufgeladen. Dies erfordert die Integration der Software-Schnittstelle des MTS in die Schwarmsubsysteme.

Unmanned Ground & Unmanned Aerial Vehicle (UGV & UAV)

Die unbemannten Roboter haben die Aufgabe das Einsatzgebiet zu erkunden, mögliche Gefahren mithilfe von Sensormessungen zu erkennen und die Einsatzkräfte mittels Bildmaterial im Einsatz zu unterstützen.

Teil der Systemarchitektur ist daher die Definition von Schnittstellen zum Roboter selbst, um eine automatische Steuerung der Bewegung zu ermöglichen, zu den Payloads des Roboters wie Sensor und Kamera und zu anderen Robotern bzw. dem MMCC.

End User

Der Endanwender ist in den von ANCHORS betrachteten Szenarien die Rettungskraft der Feuerwehr am Einsatzort. Diesem soll die Möglichkeit gegeben werden mittels des ANCHORS Systems mit dem MMCC zu kommunizieren und Daten auszutauschen.

Mission Control

Die Mission Control ist das entfernte, stationäre Einsatzzentrum der Rettungskräfte. Die Anbindung beispielsweise mittels einer Satellitenverbindung ist nicht Teil der Untersuchungen in ANCHORS.

4. AP 4 – Vehicular Ad-Hoc Communication System

Im Arbeitspaket 4 wurden verschiedenartige Kommunikationslösungen für den Rettungseinsatz untersucht. Neben der Vernetzung der Luft- und Bodenroboter stand ebenso die Gruppenkommunikation für Rettungskräfte im Fokus.

Ein wichtiger Aspekt des ANCHORS Systems ist die Robustheit des Kommunikationssystems. Diese ist essentiell für einen zuverlässigen Betrieb der Roboter in ANCHORS. Daher wurde Forschung und Experiment mit Blick auf dieses Ziel geleitet. Während der Großübung der Feuerwehr im April 2015 in Dortmund wurden zwei Kommunikationstechnologien verwendet. Zum einen wurde ein ad-hoc wireless mesh network aufgebaut, zum anderen wurde mithilfe einer mobilen LTE Basisstation eine LTE Zelle vor Ort etabliert. Die Vorteile der beiden Technologien sollten kombiniert und somit die Systemleistung gesteigert werden.

4.1 Analyse von Kommunikationsnetzen und Verhaltensoptimierung

4.1.1 Systemverhaltensoptimierung zeit-varianter Kommunikationskanäle bei Sprachkommunikation

Im Rahmen von ANCHORS wurden verschiedenartige Kommunikationstechnologien verwendet. Das wichtigste Ziel von integraler Systemplanung ist den Einfluss durch verschiedene Netze zu minimieren. Von speziellem Interesse ist Datenverkehr, die Real-Zeit Charakteristik zeigen. Das beinhaltet insbesondere Sprach-, Video und Steuerungsinformationen von UxV. Im Referenzszenario von ANCHORS wird eine Satellitenverbindung genutzt um das ‚crisis committee‘ mit den Einsatzkräften vor Ort zu vernetzen. Für die weitere Evaluation wurde diese Verbindung als ‚Black Box‘ angenommen. Dies bedingt, dass Einflüsse zwar messbar aber nicht genau identifizierbar sind.

Szenario für den Systemaufbau

Eine Annahme des ANCHORS Szenario ist der Ausfall oder Beschädigung von terrestrischen Funknetzen. Dieses Szenario basiert auf den Erfahrungen aus diversen Einsätzen in den Bereichen zivile Sicherheit und Krisenprävention. In derartigen Situationen können PMR Geräte in den sogenannten direct mode operations (DMO) Modus geschaltet werden, dadurch funktionieren die Geräte unabhängig von fest-installierter Infrastruktur. Um ein möglichst breites Spektrum an Anwendungen bereit stellen zu können müssen die Geräte im Einsatzgebiet mit der ‚core network‘ verbunden werden. Wenn der DMO Modus verwendet wird, wird ein ‚MicroSpot‘

installiert. Zusätzlich können mobile Basisstationen in das Netz eingebracht werden, allerdings müssen auch diese mit dem Kernnetz verbunden sein (siehe Abbildung 4).

Für beide Verbindungen können heterogene Transportnetze verwendet werden. In

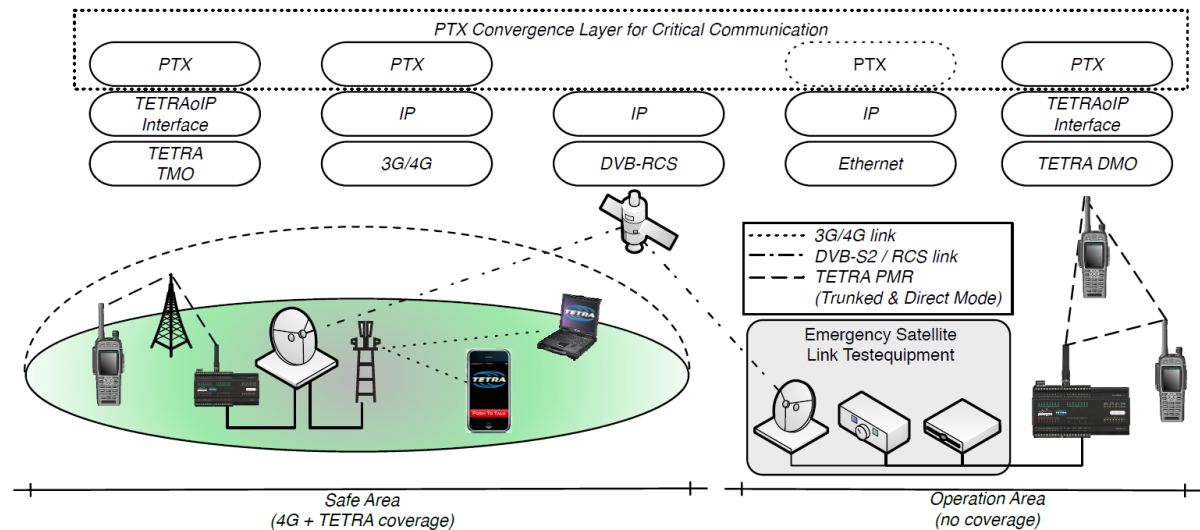


Abbildung 4: System und Schichtenstruktur [1]

Frage kommen Weitverkehrsnetze wie Satelliten oder Zellularfunknetze oder auch die Nutzung eines Wireless Mesh Networks, welches von UAVs am Einsatzgebiet bereitgestellt wird.

In vielen Fällen sind dies IP-basierte Netze, so dass der Einsatz eines QoS Gateways zwischen verschiedenen Technologien möglich ist. Im Folgenden wird daher ein IP-basierter Satellitenlink als Verbindung für TDMA-basiertes TETRA PMR Netz analysiert und getestet.

Anforderungen an Krisen-Kommunikation über heterogene Netze

Obwohl die Anforderungen variieren ist heutzutage eine zuverlässige Sprach-Gruppenkommunikation nach wie vor das wichtigste Merkmal für Krisen-Kommunikationssysteme. Steigende Geschwindigkeiten in Zellularfunknetzen vergrößern die Lücke zwischen Public Safety Communication (PSC) und kommerziellen Systemen und behindern damit zunehmend den effektiven Einsatz von PSC in Krisenfällen. Eine Möglichkeit zur Nutzung neuerer Dienste in Kombination mit bestehenden Systemen ist die Einführung eines ‚Convergence Layer‘ für PMR [1].

Convergence Layer für PMR Kommunikationsdienste

Die Basis für die vorgeschlagenen ‚Convergence Layer‘ ist das PTX¹ Protokoll. Dieses UDP/IP-basierte Protokoll ermöglicht die Nutzung von Push-Gruppenkommunikation in IP-basierten Netzen. Des Weiteren kann es als Gateway-Protokoll in einem Inter-System-Interface für TETRA dienen. Somit wird die flexible Nutzung unterschiedlicher IP-Endgeräte garantiert. Wie in Abbildung 4 zu sehen ist, ist PTX unabhängig von den darunter liegenden Transport-Protokollen. Es bietet ein call-handling und Gruppenmanagementfunktionen ohne zusätzlicher Overhead in der Kommunikation zu verursachen, da der Header nur eine Größe von einem Byte aufweist.

Ein weitere Funktion von PTX ist die Realisierung von Kommunikationsoptionen wie ‚cross layer controlling‘ von Gateways. Dies ist insbesondere dann wichtig, wenn es keinen vollen Zugriff auf die unteren Schichten des Protokollstacks gibt.

Adaptive Multiplex Gateway für TETRA over IP Dienste

Wie in den vorangegangenen Abschnitten dargelegt ist die Steuerung und Optimierung der unteren Schichten eines Protokolls in heterogenen Umgebungen notwendig. In Abbildung 5 wird das klassische Modell einer Sprachübertragung gezeigt. Es ist in drei Aspekte geteilt: den Sender, dem Übertragungskanal und dem Empfänger. Das Ursprungssignal der Quelle (z.B. Mikrophon) wird mit einer Sampling Rate $f_s = 162/3 \text{ Hz} \approx 60 \text{ ms}$ digitalisiert. Diese Frequenz ist das Slot-Intervall von TETRA TDMA Systemen und wird gewählt um die Interoperabilität zwischen IP und PMR Netze zu gewährleisten. Die Parameter des kommerziell-betriebenen Satelliten sind nicht verfügbar und daher als Kombination zweier Verzögerungsglieder ($\tau_{channel}, \tau_{jitter}(t)$) sowie zweier Fehlerraten (Paket- und Bitfehler) beschrieben. Der Empfänger wird mit einem zusätzlichen Empfangsspeicher ausgestattet um auf die zeitvariante Verzögerung (Jitter) zu reagieren.

Ein zusätzlicher Speicher und Bytes sind für den Sender vorgesehen. Beide Manipulationen des originären Datenstroms werden durchgeführt um das Verhalten des Übertragungskanals zu studieren. Hinzu kommt, dass Satellitensignale anfällig sind für hohe Paketfehlerraten (packet error rates – PER). Für die beabsichtigte Integration von Satellitenkanälen in TETRA-Netze ist eine PER von bis zu 10% akzeptabel ohne die QoE² zu reduzieren. Daher wird dieser Wert als Grenze für einen erfolgreichen Verbindungsaufbau im Messaufbau verwendet.

¹ Push-To-X <http://openptx.org>

² Quality-of-Experience

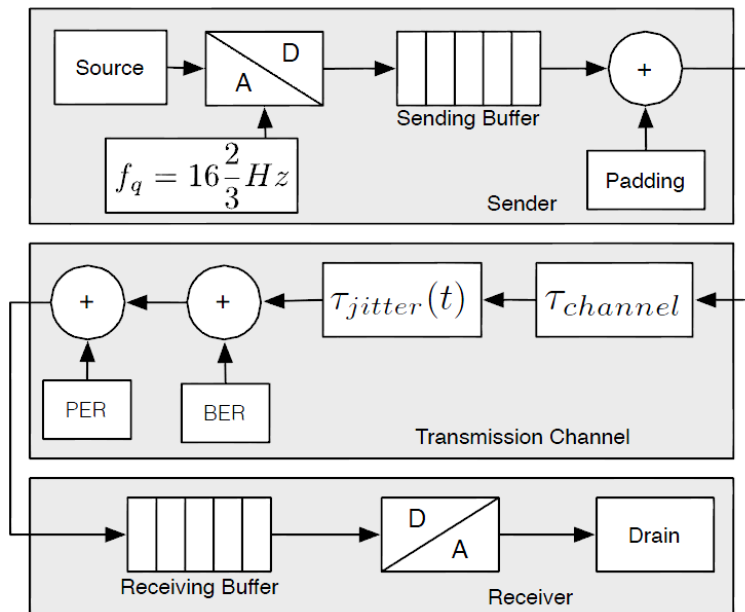


Abbildung 5: Modell einer Übertragung [1]

Kanäle kommerzieller Satellitensysteme sind im Allgemeinen nicht auf eine Minimierung des Jitter im Datenstrom ausgerichtet. In den meisten Fällen wird daher ein interner Sende-Puffer verwendet um kurze Sprünge im Up-Link zu vermeiden. Dieser Puffer führt zu einem Jitter $\tau_{jitter}(t)$. Im beschriebenen Modell würde eine Vergrößerung der Paketgröße das System dazu zwingen alle Pakete direkt zu

senden, was zu einer Verkleinerung des Jitter führen würde. Ein optimales Verhalten wird bei der maximalen Transferrate angenommen. An diesem Punkt werden alle potentiellen Puffer neutralisiert.

Da die Struktur der Information bzgl. Sampling Rate und Paketgröße unveränderlich ist, bleiben wenige Optionen um die Kanalbedingungen zu optimieren:

1. Speichern von n Paketen um größere Pakete zu erstellen (Jumbo-Pakete)
2. Erhöhen der Paket-Größe durch Hinzufügen von Füll-Bytes
3. Größere Pakete kreieren durch Multiplexing von mehreren Sprach-Transmissionen in einen Übergangs-Transmission-Datenstrom.

Lösung 1) ist durchführbar wird allerdings zu einem Anstieg der Verzögerung führen und dadurch die maximale Paketgröße PS beschränken. Die Option 2) ist flexibel, wird die Paketverzögerung nicht erhöhen und eröffnet die Möglichkeit für Bytegrößen Anpassung. Der Nachteil die große Reduzierung der Datenrate.

Um den Vorteil der beschriebenen Option zu erhalten und gleichzeitig die negativen Effekte zu minimieren, wird die Nutzung eines adaptiven Multiplexer vorgeschlagen. Der Multiplexer erzeugt größere Datenpakete, die mehrere Sprachpakete enthalten ohne die Verzögerung oder den Overhead zu erhöhen. Wenn der anliegende Verkehr nicht groß genug ist, wird fehlende Bytes aufgefüllt. Dieser Multiplexer muss als Gateway Dienst in der ganzen Systemarchitektur eingeführt werden. Die zusätzliche PTX-Signalisierung und Steuerung der Schnittstellen ermöglicht die adaptive Änderung der Sendeparameter um auf unterschiedliche Kanalbedingungen zu reagieren. Diese Feedback-Schleife ist wichtig um eine Überlastung und somit eine Erhöhung der PER zu vermeiden. Die Signaling-Information kann innerhalb ungenutzter Slots im Multiplex-Stream oder als Overhead gesendet werden. Eine

kontrollierte Überlast kann aber auch genutzt werden um die Kapazität des Transportlinks zu erhöhen. Vorangegangene Arbeiten zeigen, dass ACELP-kodierte Sprache bis zur PER von 10% verständlich ist. Wenn das Multiplexing-Gateway eine Überlast detektiert, kann der Fehler zwischen verschiedenen Datenströmen aufgeteilt um eine Gleichverteilung der Fehler zu erreichen.

Auf Client-Seite ist die Nutzung dieses Gateways transparent innerhalb des ‚convergence layer‘ und wird somit nur durch eine Reduzierung des gemessenen Jitters und der resultierenden Puffergröße bemerkt. Die Überwachung der Inter-Arrival-Time der Pakete beim inversen Multiplexer verhindert Überlast-Situationen.

Leistungsevaluation

In der Leistungsanalyse wird der Fokus auf die Korrelation zwischen dem Jitter einer Sprachverbindung mit der tatsächlichen Paketgröße, die von einem Multiplex-Gateway-Service kontrolliert wird, gelegt. Um die Nutzbarkeit zu garantieren wird die Round-Trip-Time (RTT) eines Verbindungsaufbaus unter den gleichen Bedingungen gemessen. Alle Tests wurden mindestens 50-mal durchgeführt um externe Einflüsse auszuschließen. Die mittels Push-To-Talk erzeugten Sprachnachrichten haben eine Länge von mindestens 10 Sekunden.

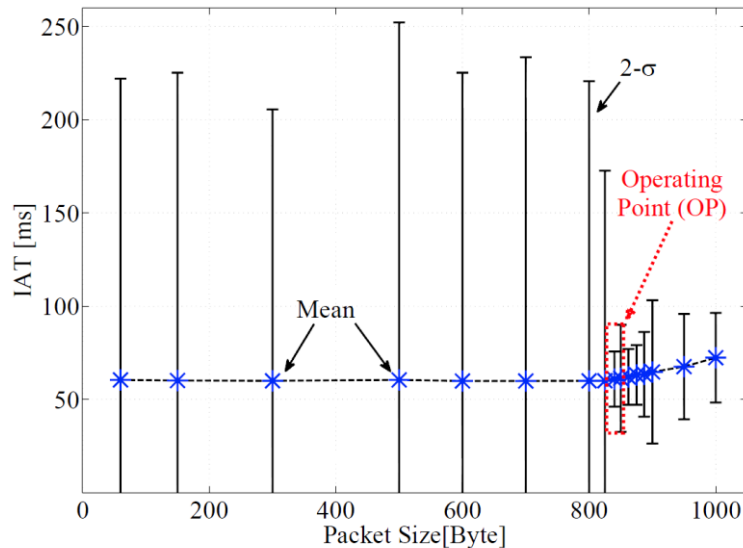


Abbildung 6: Optimierter Jitter durch Erhöhung der Paketgröße [1]

Messaufbau – Emergency Satellite Link Test Equipment (ESLT)

Um die Leistung und womöglich auftretende Effekte der vorgeschlagenen Lösung objektiv untersuchen zu können, wurde ein sogenanntes Emergency Satellite Link Test Equipment (ESLT) aufgebaut. Dieses ist mobil und beinhaltet eine Stromversorgung, einen WiFi-Router (IEEE 802.11n) sowie ein Antennenkontrollsystem um automatisch nach Satelliten suchen zu können.

Jitter Analyse

Bei Sprachkommunikation soll die Schwankung der IAT so klein wie möglich sein. Im betrachteten System werden Pakete der Größe 60 Byte alle 60 ms gesendet. Wie in Abbildung 6 zu sehen ist, ist der Mittelwert der IAT konstant, weist allerdings einen hohen Jitter auf. Die 2σ Standardabweichung zeigt, dass der Empfangspuffer mit IAT von bis zu 250 ms umgehen können muss.

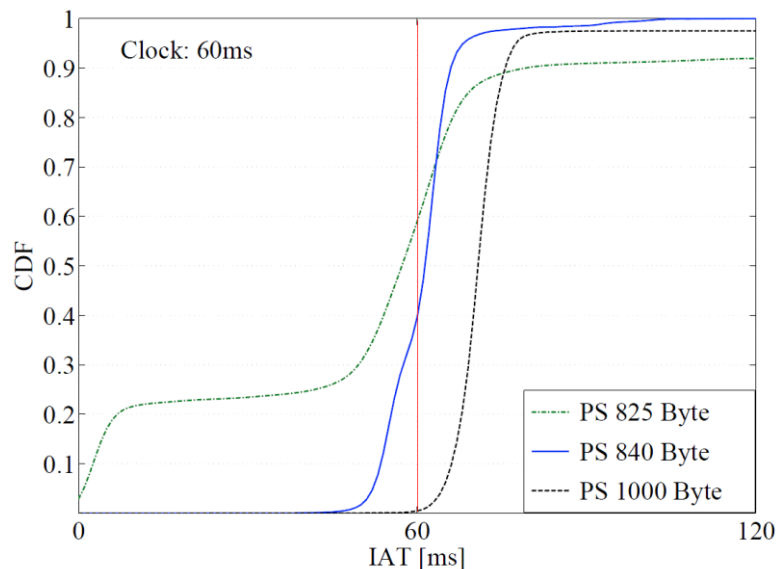


Abbildung 7: IAT Analyse für unterschiedliche Paketgrößen [1]

Im vorangegangenen Kapitel wurde ausgeführt, dass die beste Systemleistung bei einer Verkehrslast von 100% erreicht wird. Um diesen Operating Point (OP) zu identifizieren wird die Paketgröße stetig erhöht. Die Messungen zeigen einen optimalen OP bei einer Paketgröße von 840 Bytes. Dies führt zu einer effektiven Upload-Datenrate von 112 kbit/s. Bei weiterer Erhöhung der Paketgröße kann ein Einsteigen der IAT festgestellt werden.

Dieser Effekt ist in Wahrheit bedingt durch den Anstieg der Paketfehlerrate, verursacht von einer Überlast des Links. Verglichen mit der ursprünglichen Paketgröße wurde der Jitter um den Faktor 11 reduziert. In Abbildung 7 wird eine detaillierte CDF Analyse präsentiert. Es ist zu sehen, dass beim OP die reale IAT nahe am Idealwert von 60 ms ist. Insbesondere im Gegensatz zu kleinen Paketgrößen konnte ein optimales Systemverhalten erreicht werden. In Abbildung 8 wird die resultierende Verzögerung dargestellt. Die Round-Trip-Time (RTT) eines Rufaufbaus steigt mit zunehmender Paketgröße. Dies kann toleriert werden, da die Verzögerung einen kleineren Einfluss auf die Qualität der Sprachkommunikation hat im Vergleich zum Jitter.

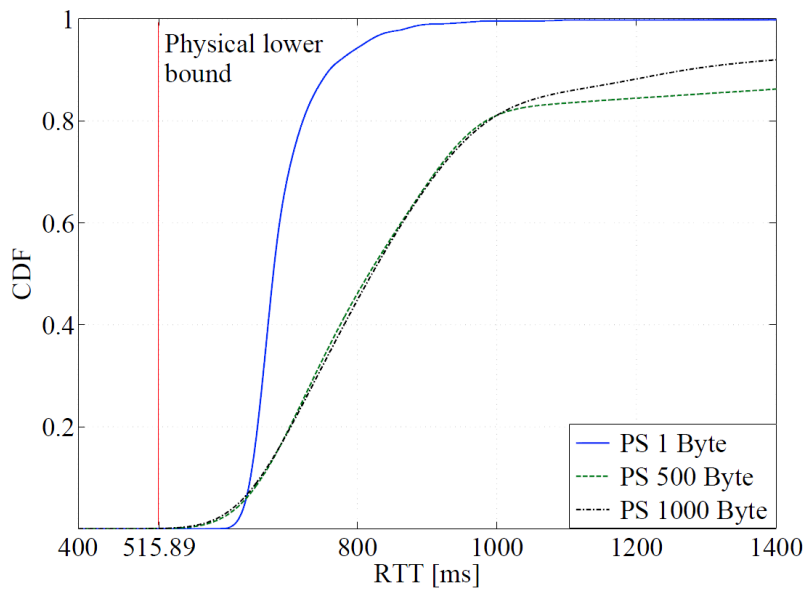


Abbildung 8: RTT Analyse eines Rufaufbaus für unterschiedliche Paketgrößen [1]

4.1.2 Active Delay Management (ADeM) für Gruppenkommunikation über heterogene öffentliche Zellularkommunikationsnetze

Während der vergangenen Jahre wurden Terrestrial Trunked Radio (TETRA) Systeme zu einer zuverlässigen Kommunikationslösung für Rettungskräfte. TETRA ermöglicht sowohl eine sichere Sprachkommunikation als auch niederbitratige Datendienste (vergleichbar zu 2G Zellularkommunikationsnetzen). Auf der anderen Seite bieten öffentliche Zellularkommunikationsnetze ihren Nutzern eine heterogene Netztopologie (2G, 3G and 4G) mit

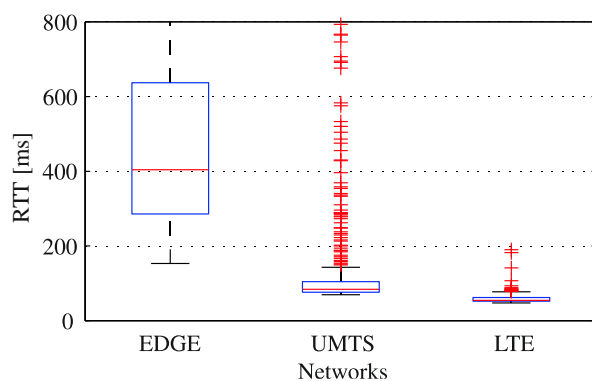


Abbildung 9: Statistische Verteilung von RTT in zellularen Funknetzen im urbanen Raum [5]

nahezu weltweiter Abdeckung, hohen Datenraten und einer Verfügbarkeit von nahezu 100%.

Dies bewirkt den Wunsch von Sicherheitsbehörden die gleichen Dienste in ihren Kommunikationsnetzen zu bekommen. Diese Anforderung kann erfüllt werden wenn Gateways zwischen verschiedenen Kommunikationsnetzen (heterogene, kommerzielle Netze oder sichere TETRA Netze) verwendet werden um die Lücke zwischen den Netzen zu schließen und die Vorteile zu kombinieren.

Eine große Herausforderung in diesem Kontext ist der Einfluss von heterogenen Technologien auf die Verzögerung und den Jitter der übertragenen Daten. Die Abbildung 9 zeigt die statistische Verteilung der Round-Trip-Times (RTT). Demnach ist offensichtlich, dass aktuelle 4G Netze wie LTE eine kleinere Verzögerung als 2G (GSM) oder 3G (UMTS) aufweisen. Da in TETRA Systemen das Prinzip „push first – talk first“ während des Rufaufbaus gilt, kann ein unfaires Systemverhalten beobachtet werden. Nutzer, die in 4G Netzen operieren haben eine signifikant höhere Chance für einen erfolgreichen Rufaufbau als Nutzer in 2G oder 3G Netzen, die alle zur gleichen Zeit einen Sendewunsch haben. Zudem gilt, dass eine Sprachkommunikation über heterogene Netze wegen der hohen Anforderungen an einen tolerierbaren Jitter sehr herausfordernd ist. Die Qualität der Sprachübertragung leidet unter großen Varianzen in der Übertragungsverzögerung. Beide Probleme verursachen unzuverlässiges Systemverhalten, welches letztendlich zu einer geringen „Quality-of-Experience“ für den individuellen Benutzer führt.

Dieses Verhalten kann vermieden werden, wenn ein “Active Delay Management (ADeM)” [5] integriert wird. Die Abbildung 10 veranschaulicht die Struktur eines Systems, welches heterogene Technologien und die ADeM Architektur kombiniert (PSP IP Active Gateway).

ADeM adressiert zwei Ziele: Optimierung des Jitter um die Qualität der Sprachübertragung zu erhöhen und die Fairness des Systems. Beide Ziele werden erreicht indem ein sogenanntes „Active Queue Management (AQM)“ mit entsprechenden Puffern verwendet wird.

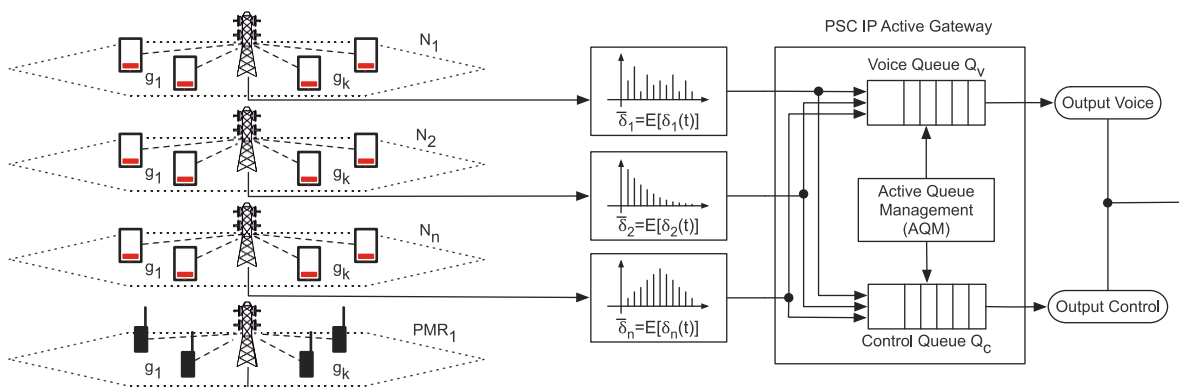


Abbildung 10: Public Safety Communication Systeme mit integrierter ADeM-Architektur [5]

Ein Sprachpuffer Q_v hilft den Jitter zu optimieren. Die Herausforderung ist die Wahl der Puffergröße: ist er zu klein, kann ein nicht-tolerierbarer Jitter auftreten, ist er zu groß, können die Verzögerungen zu groß werden. Die Verbesserung der System Fairness für den gleichzeitigen Rufaufbau von Wettbewerbern wird durch die Einführung des Kontroll-Puffers Q_c realisiert. Dieser Puffer stellt die gleiche Verzögerung für alle Rufaufbau-Pakete unabhängig von der verwendeten Technologie her. Dafür fügt der Kontroll-Puffer eine zusätzliche Verzögerung zu allen einkommenden Paketen hinzu. Der Wettbewerber mit der höchsten Verzögerung bestimmt den Wert. Das verursacht größere Verzögerungen für Datenpakete aus 4G-Netzen im Vergleich zu Datenpaketen, welche aus 2G bzw. 3G-Netzen kommen.

Beide Teile von ADeM arbeiten indem sie nur die Klassifizierung der Netztechnologie der einkommenden Datenpakete nutzen. Diese Klassifizierung wurde bereits vorgestellt und weist eine Erfolgsrate von 95% auf.

Die Abbildung 11 zeigt die Ergebnisse der Simulation für das beschriebene System. Es wird deutlich, dass der Fairness-Index des Systems und damit die Anzahl der

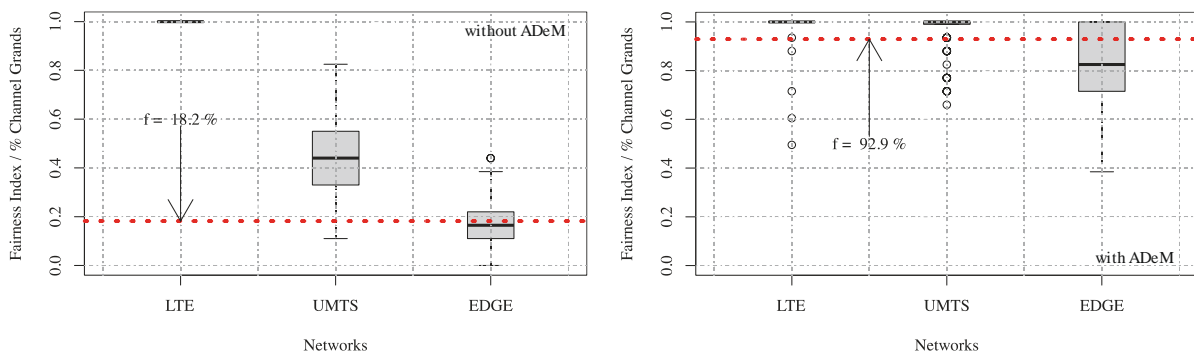


Abbildung 11: Die Verteilung der Fairness des betrachteten Systems ohne (linke Seite) und mit (rechte Seite) Integration von ADeM [5]

erfolgreichen Rufaufbauten im Verhältnis zu Gesamtzahl der Versuche mit der Anwendung von ADeM von 18,2% auf 92,9% gesteigert wird.

4.1.3 Verteilte Flusskontrolle bei Missionskritischer Kommunikation

Die ersten Analysen von Multihop Relaying am Boden zeigte die Schwierigkeiten der Schwarmrobustheit bei der Verwendung von aktuellen Lösungen. Wenn UAVs oder

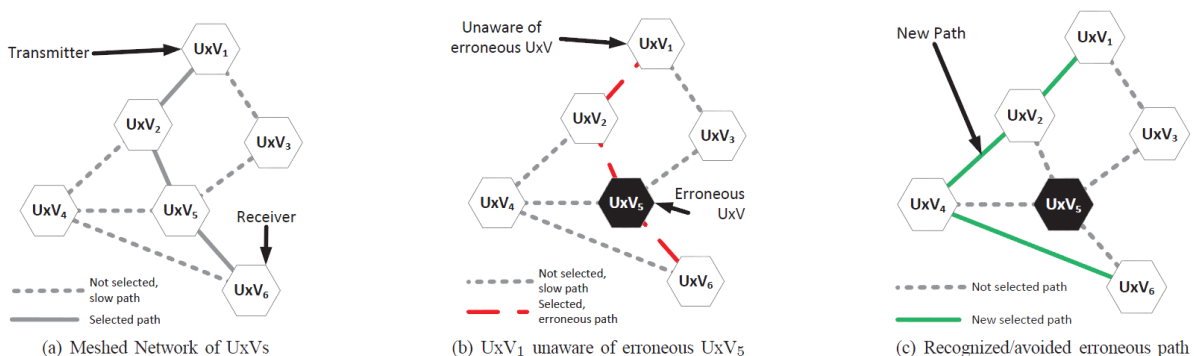


Abbildung 12: Schwierigkeiten aktueller Ansätze bzgl. Schwarmrobustheit [6]

UGVs fehlerhaft arbeiten, können Aufgaben unter Umständen nicht mehr erfolgreich durchgeführt werden und das Schwarmverhalten wird negativ beeinflusst. Die Abbildung 12 veranschaulicht das Problem. Der Schwarm verwendet ein dediziertes Wireless Mesh Network (WMN), welches von Applikationen mit Kontext-abhängigen Leistungsanforderungen (vgl. Abbildung 12(a)) genutzt wird. In diesen Netzen ist die Differenzierung der Applikationen der Schlüssel um ein Multiplexing und eine Bewertung der Datenströme hinsichtlich ihrer Leistungsanforderungen zu ermöglichen und somit die beschränkten Ressourcen optimal zu nutzen. Um eine Verkehrsbewertung durchzuführen, werden die Verkehrsströme einmal beim ersten Hop eines WMN klassifiziert und gekennzeichnet, um eine schnelle Identifizierung, Differenzierung und Bewertung bei nachfolgenden Knoten zu ermöglichen.

Die Genauigkeit der Identifizierung hängt von den zur Verfügung stehenden Paket-Header Informationen ab. Dies ist kritisch, da die Pakete zum Teil verschlüsselt sind. Obwohl es zahlreiche Ansätze gibt diese Probleme in Teilen zu lösen, sind diese Ansätze nicht dafür geeignet mit den beschränkten Ressourcen eines Eingebetteten Systems eines UAVs umzugehen. Da eine zuverlässige Datenübertragung unerlässlich für eine erfolgreiche Missionsdurchführung ist, muss die Güte der Identifizierung verbessert werden. Deswegen sollte die Klassifizierung eines Datenstroms am Ursprungsort jedes Stroms erfolgen. Jedoch macht ein Defizit diese Architektur verwundbar: der Ursprungsknoten könnte selbst hohe Priorität für seine eigenen Datenströme verwenden. Dies könnte die Folge von fehlerhaftem Verhalten oder eines internen Angriffs sein, der die eigenen Datenströme bevorteilt ohne die Gesamtmission zu beachten. Weiter gilt, dass auch Relaying-Knoten fehlerhaft arbeiten könnten und beim Weiterleiten die Datenströme anderer Knoten beschädigen (vgl. Abbildung 12 (b)). Wenn die UxVs verschiedener Rettungsorganisationen zusammengeführt werden können die beschriebenen Probleme auftauchen und zu einer Leistungsminderung der Datenübertragung führen. Bisher vorgestellte Sicherheitslösungen für derartige Systeme betrachten nur die Authentifizierung der Knoten und Datenintegrität. Daher wird das Distributed Flow Permission Inspection (DiFPIN) [6] vorgestellt um die Schwarmrobustheit zu verbessern und dennoch die Klassifizierung beim Ursprungsort durchzuführen. In der Folge kann fehlerhaftes Verhalten und interne Attacken erkannt, die Nutzung fehlerhafter Pfade (vgl. Abbildung 12 (c)) vermieden und die Leistungsfähigkeit damit erhöht werden.

Das Ziel von DiFPIN ist den negativen Einfluss von fehlerhaften Knoten und internen Angreifern auf einen Schwarm von UAVs zu reduzieren. Der Klassifikationsprozess ist dezentralisiert, das System wird auf jeden UAV eingesetzt um ständig die Klassifizierung am Ursprungsort zu ermöglichen.

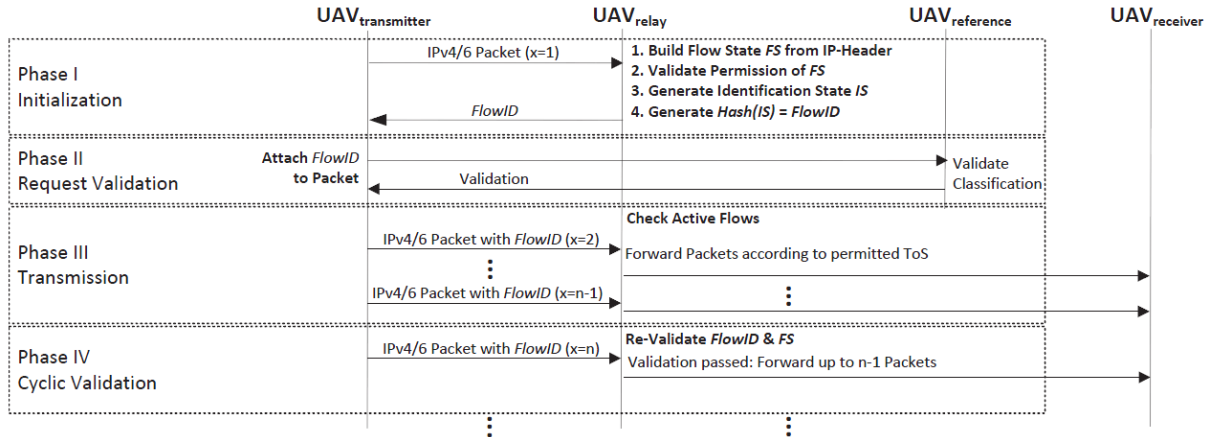


Abbildung 13: Die unterschiedlichen Phasen des DiFPIN Schemas [6]

DiFPIN besteht aus vier Phasen (vgl. Abbildung 13): In der Initialisierungsphase wird eine Handshake zwischen dem Sender und einem Relay durchgeführt, in welchem die Erlaubnis des Sende-Stroms und das ToS (Type-of-Service) Feld validiert werden. Dies wird durch die Übertragung einer FlowID bestätigt. Um auch diese FlowID ihrerseits zu überprüfen nutzt der Sender einen dritten, unbeteiligten Knoten als Referenzknoten. Nach der positiven Bestätigung beginnt die Übertragung in der dritten Phase des Schemas. Die FlowID wird zu jedem Datenpaket hinzugefügt, beides wird im Relaying UxV geprüft und dann je nach ToS-Wert weitergeleitet. Die FlowID wird in Form einer LookUp-Table organisiert, der Vergleich kann somit schneller durchgeführt werden als wenn jedes Mal alle Paketinformationen betrachtet werden müssen. Zudem ist dieser Weg zuverlässiger als die ausschließliche Betrachtung des Wertes des ToS-Felds. Um Missbrauch zu vermeiden wird jedes n-te Paket geprüft in Form einer zyklischen Validierung. Wird dieser Test bestanden, dann werden auch die nächsten n-1 Pakete versendet. Falls der Test nicht bestanden wird, werden die Pakete zwar auch weitergeleitet, werden jedoch nur wie best-effort Pakete behandelt. Der Cross-Check zwischen den UxVs erlaubt die Detektion und somit den Ausschluss von fehlerhaften oder attackierten UxVs aus dem Pfad.

Eine wichtige Anforderung ist, dass ausreichend Informationen für eine Klassifizierung zur Verfügung stehen. Die erforderlichen Informationen können aus dem IPv4 und TCP/UDP Header jedes Pakets abgeleitet werden, ein zusätzlicher Overhead ist daher nicht notwendig. Die Informationen werden genutzt um einen Flow State FS zu erstellen, der Signatur der Applikation $APPSig$ und den Type of Service ToS enthält:

$$FS := APPSig, ToS$$

Die Dienstsignatur wird durch die Ziel IP (*destIP*) einer Transmission, den Port der Transportschicht am Ziel und das verwendete Protokoll definiert:

$$APPSig := DestIP, Port, Protocol$$

Aus Effizienzgründen wird ein Hash des Flow State *FS*, genannt *FlowID*, verwendet. Als erstes wird ein Identification State *IS* generiert, Dafür wird der Flow State *FS* gegen eine UxV und Strom-individuelle *NONCE* (number used once) gerechnet um die Neuheit jeder *FlowID* zu garantieren:

$$IS := FS \oplus NONCE$$

$$FlowID := HASH(IS)$$

Mit den durch Flow State *FS* gegebenen Informationen hat der eingebettete bit string eine Länge von 64 bits. Das Oktett dieses und des personalisierten bit strings werden summiert und mit modulo *n* verrechnet. Die Anzahl der Permutationen für diesen bit string richtet sich nach einer Zufallsverteilung, die von der Anzahl der UxVs und der Anzahl der Dienste abhängt. Die Auswahl der Verteilung ändert sich mit der Anzahl der Permutationen innerhalb des Oktetts und muss an die Sicherheitsanforderungen des Szenarios angepasst werden:

$$f_{hash}(IS) := \sum_{octets} IS \bmod n$$

Für eine allgemeine Definition wird *n* durch die Differenz zwischen maximalen und minimalen Hashwerten innerhalb der Verteilung bestimmt:

$$n := \frac{|Max_{f_{hash}(IS)}| - |Min_{f_{hash}(IS)}|}{\sigma(f_{hash}(IS))}$$

Nach der abstrakten Beschreibung von DiFPIN folgt die detaillierte Funktionsweise. Alle erlaubten Konfiguration von Paket-Headern eines UxV werden in einer Permitted Configuration List (PCL) verwaltet. Diese wird a Priori von allen UxVs erstellt. Jedes UxV verwaltet daher eine Tabelle mit Zuordnungen eines FS zu einer Konfiguration:

$$tuple_{pt} := FS_m \rightarrow PCL(UxV_n)$$

Wenn das erste Datenpaket ein Relaying-UxV erreicht muss der Flow State *FS* mindestens einem Tupel dieser Tabelle zugeordnet werden können um korrekt validiert und klassifiziert zu werden. Ist dies nicht der Fall, wird dieses und alle nachfolgenden Pakete dieses Datenstroms nach dem Best-Effort Verfahren weitergeleitet.

In einem Szenario mit einem fehlerhaft operierenden UxV wird der Grad der Robustheit reduziert. Um ein höheres Sicherheitslevel zu erreichen wird der Kommunikationsprozess in einer zweiten Phase weiter validiert. Dazu wird die *FlowID* an einen dritten, bislang unbeteiligten Knoten geschickt. Dieser Knoten sollte die gleiche *FlowID* generieren können, ist dies nicht der Fall, arbeitet einer der Knoten fehlerhaft.

Für die Evaluierung wird der Quality of Robustness Indicator $QoRI$ eingeführt. Der $QoRI$ beschreibt die Robustheit eines WMN und bietet somit die Möglichkeit die Verbesserung durch DiFPIN in Szenarien mit gegebener Robustheit zu quantifizieren. Die Abbildung 14 zeigt die queuing time für ein Szenario mit einem gegebenen $QoRI = 0.5$. Die Resultate unterstreichen, dass die Leistung einer Missionskritischen Übertragung deutlich von der höheren Robustheit gegenüber den Gefahren, die durch

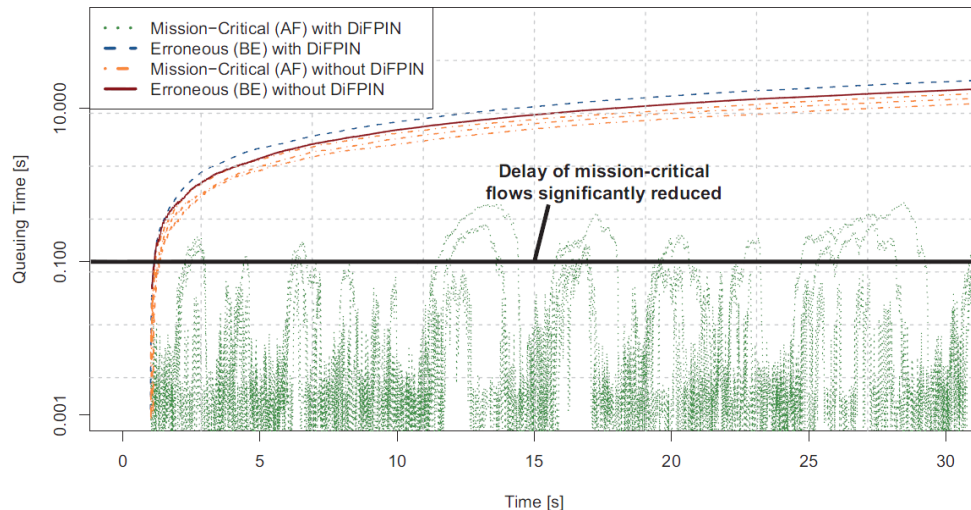


Abbildung 14: Durchschnittliche Wartezeit für ein Szenario mit $QoRI = 0.5$ [6]

DiFPIN adressiert werden profitiert. Wenn die Robustheit des Netztes auf einen $QoRI$ von 0,3 fällt, dann werden die Grenzen des Ansatzes deutlich. DiFPIN kann also die Leistungsfähigkeit positiv beeinflussen, benötigt allerdings eine Mindest-Robustheit des Systems.

4.2 Content-aware Hybrid Communication System Design

In der Mehrheit der bislang betrachteten UAV Szenarien wurde eine Technologie für die Kommunikation genutzt. Dies ist verbunden mit mehreren Problemen:

- *Geringe Ressourcenverfügbarkeit* – Funkspektrum ist beschränkt, verfügbare Frequenzbänder sind evtl. nicht ausreichend um alle Anforderungen zu erfüllen
- *Interferenzen* – Falls das ISM-Band genutzt wird, können Kollisionen mit anderen Nutzern auftreten
- *QoS Anforderungen nicht erfüllt* – Nutzung einer Technologie unzureichend hinsichtlich Anforderungen

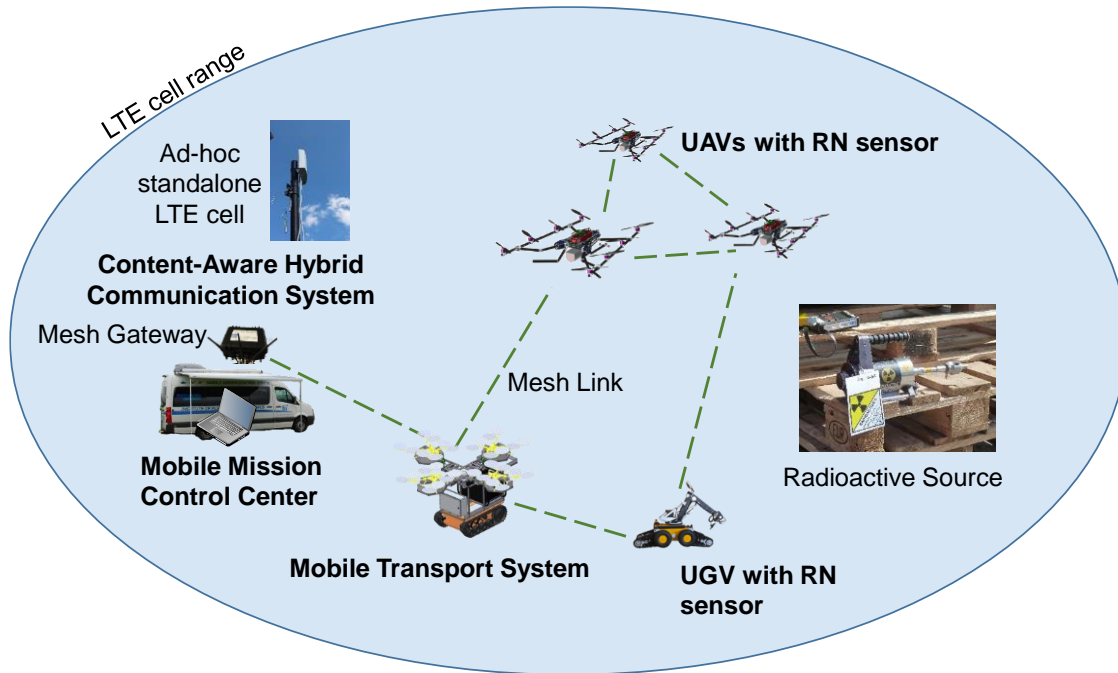


Abbildung 15: Konzept des Content-aware Hybrid Communication (Quelle: TU Dortmund)

Eine Lösung für die genannten Probleme ist die Einführung der Content-aware Hybrid Communication. Die Idee ist es die Vorteile verschiedener Kommunikationstechnologien zu bündeln und damit die folgenden Ziele zu erreichen:

- *Reichweite (Multi-hop vs. zentralisiertes System)* – Hohe Reichweite in Zellularfunknetzen
- *Ressourcenmanagement (QoS in LTE)* – QoS management in Zellularfunknetzen
- *Erhöhter Durchsatz* – durch parallele Verwendung mehrerer Technologien
- *Kein Single-Point-of-Failure (WLAN-Mesh)* – in einem Multi-hop Netz sind meist mehrere Routen verfügbar



Abbildung 16: HD-Bildübertragung während der ANCHORS Übung (Quelle: TU Dortmund)

In ANCHORS werden LTE und Wireless Mesh Networks genutzt. Die übermittelten Daten werden auf beide Technologien aufgeteilt. Während der Durchführung einer Mission werden folgenden Verkehrstypen verwendet:

- *Telemetry information* – Alle Roboter senden ihren aktuellen Status, z.B. GPS Information, Akkustand etc. zum MMCC und zu den anderen Robotern im Netz.
- *Mission control data* – Der Missionsoperator sendet aktuelle Kommandos oder neue Wegpunkte zu den Robotern.
- *Sensor data* – In ANCHORS wird ein Nuklearsensor verwendet, dessen Daten werden zum MMCC gesendet um potentielle Gefahren und ihre Ursachen zu finden.
- *Multimedia data* – Vielfach sind die Roboter mit Kameras ausgerüstet um dem Missionsoperator Bild- und Videoinformation zu liefern.

Wenn der Inhalt dieser Daten betrachtet wird, ist offensichtlich, dass hier verschiedene QoS Anforderungen zur Anwendung kommen. *Mission control data* muss mit geringer Verzögerung, *multimedia data* benötigt hohe Datenraten. Daher soll für jeden Verkehrstyp die richtige Kommunikationstechnologie ausgewählt werden (vgl. Abbildung 17).

4.2.1 Content-aware Hybrid Communication System Architektur

Der erste Schritt zu einem Content-aware Hybrid Communication System ist die Integration aller Technologien und potentiellen Datenquellen in das ANCHORS System Framework. Die UxV System Development Platform of ANCHORS wird in den vorherigen Abschnitten ausführlich vorgestellt. Damit wird die Missionssteuerung und die Schwarmoperationen ermöglicht, weiter wird aber auch jede Kommunikation dadurch gesteuert. Die Abbildung 17 verdeutlicht die Ideen hinter der Hybrid

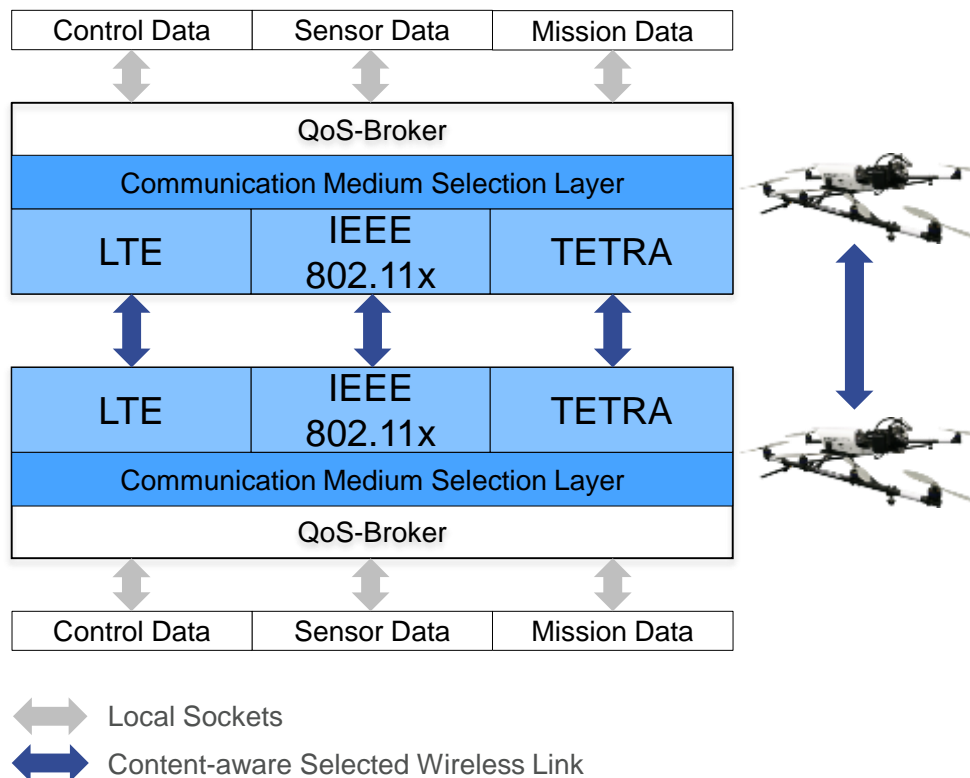


Abbildung 17: Architektur des Content-aware Hybrid Communication Systems
(Quelle: TU Dortmund)

Communication System Architektur. Die Sensoren, Kameras und andere Payload ist local auf dem Fluggerät mittels serieller Schnittstellen angebunden. Alle anfallenden Daten werden durch den *QoS-Broker* analysiert. Die Aufgabe dieses Brokers ist die Datenpakete zu speichern und zu klassifizieren. Diese Klassifizierung wird genutzt um mittels zuvor definierten Scheduling-Algorithmen im *Communication Medium Selection Layer* zu entscheiden welche Technologie genutzt wird. Zusätzlich zu der Analyse der Daten werden die aktuellen Bedingungen auf jedem verfügbaren Kommunikationskanal gemessen. Mit der Hilfe von kleinen Testnachrichten wird die Round-Trip-Time (RTT) bestimmt, diese wird ebenso wie die Nutzung der Puffer in die Entscheidung mit einbezogen.

Das Design von Scheduling-Verfahren ist ein interessanter und wichtiger Forschungsaspekt. In ANCHORS werden zwei grundlegende Verfahren verwendet:

1. *Load balancing* – Mithilfe eines sogenannten Round-Robin Verfahren werden die Daten alternierend auf beide Technologien aufgeteilt.
2. *Robustness* – Um die Robustheit und die Stabilität des Systems zu erhöhen, werden alle Datenpakete dupliziert und über beide Technologien gesendet.

Das Kommunikationssystem wird kontinuierlich durch die CNI Ground Station überwacht wie in Abbildung 18 zu sehen ist. In diesem Testfall ist der SCA (und damit das UAV) über Ethernet und WLAN mit dem SCG verbunden.

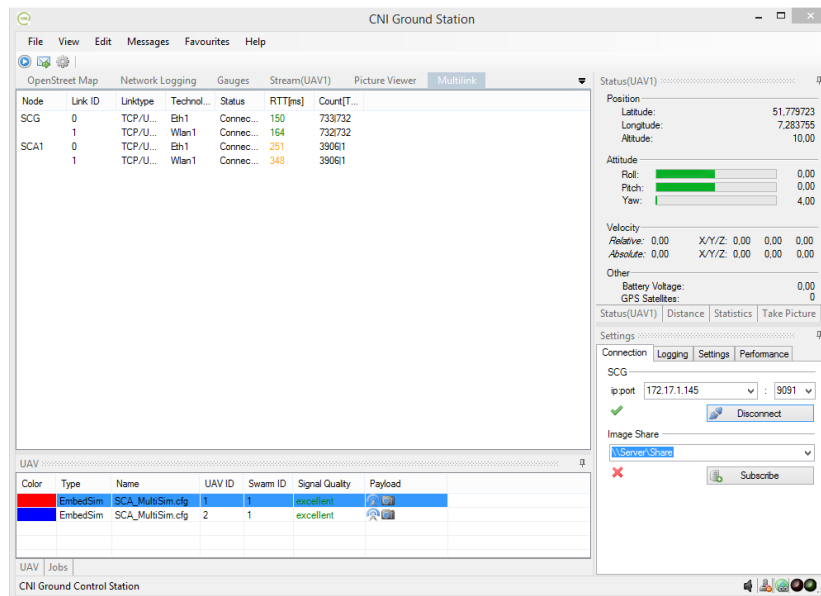


Abbildung 18: Monitor Hybrid Communication System (Quelle: TU Dortmund)

4.3 Mobile Ad-hoc LTE Zellen

Die Verwendung der Technologie von LTE Funknetzen in Krisensituationen bietet zahlreiche Vorteile. Zunächst ist festzuhalten, dass die Technologie für große Reichweiten (mehrere Kilometer) bei gleichzeitig hohen Datenraten (mehrere Mbit/s) ausgelegt ist. Zudem ist eine anerkannte Authentifizierungstechnik (SIM Karten) integriert. Zentrales Funkressourcen Management wird verwendet um Datenkollisionen zu vermeiden und eine hohe spektrale Effizienz zu erzielen. Die Nutzung eines lizenzierten Frequenzspektrums verhindert Störungen und Interferenzen durch andere Nutzer wie dies im unlizenzierten ISM-Band häufig auftritt. Als IP-System konzipiert, bietet LTE einen schnellen und effizienten Datentransfer durch das Netz.

Die Verfügbarkeit von günstigem User Equipment (UE) wie USB-LTE-Modems ermöglicht die schnelle Skalierbarkeit als auch den schnellen Austausch von beschädigten Komponenten.

Um ein LTE Netz aufzubauen sind drei Hauptkomponenten erforderlich. Als erstes wird ein LTE Core Network (Evolved Packet Core, EPC) benötigt. Dies ist üblicherweise

ein Landesweites Netz verschiedener Komponenten kann aber auf die Größe eines (embedded-)PC minimiert werden und betreibt die benötigten Grundfunktionen des LTE Kerns. Zweite Komponente ist die Basisstation (in LTE eNodeB genannt), die das LTE Zugangsnetz aufspannt und zum EPC verbunden ist.

Die Basisstationen werden üblicherweise von kommerziellen Anbietern an einen Ort stationär angebracht und können mit hoher Leistung senden. Daher sind die Geräte meist schwer und groß. Dennoch können sie in einem Wagen der Rettungskräfte integriert werden.

Als drittes wird das UE benötigt, dies wird mit einer für das Netz gültigen SIM Karte ausgestattet.

Um die Größe, das Gewicht und die Kosten der Basisstation zu reduzieren können auch Software Defined Radios (SDR) verwendet werden. Damit kann der Einsatz von LTE Femto Zellen in Krisensituationen wie nachfolgend beschrieben evaluiert werden.

4.3.1 System Design für mobile LTE Zellen

Im betrachteten Krisenszenario wird ein dediziertes LTE Netz verwendet um alle Roboter und das MMCC durch einen zusätzlichen Link miteinander zu vernetzen. Zu diesen Zweck wird das Netz wie in Abbildung 19 zu sehen aufgebaut. Alle beschriebenen Subnetze haben die Subnet Mask 255.255.255.0. Das Netz besteht hauptsächlich aus zwei physikalischen Computern, einem LTE EPC und einem VMWare-Server (dieser betreibt einen VPN Server und einen Router). Diese sind mittels eines Ethernet-Switch mit einem eNodeB (NSN Flexi Cell) verbunden, hinzu kommt die optionale Internetanbindung, in Feuerwehrübung durch einen Satellitenlink realisiert. Der LTE EPC realisiert die benötigten LTE Core Network Komponenten, wie z.B. Authentifizierung, Zugang und die Kapselung des Datenverkehrs für den LTE Transportlink. Daten vom UE werden durch LTE Schnittstellen und Tunnel geleitet und verlassen das EPC nach einer Network Address Translation (NAT) durch das Serving Gateway Interface (SGI). Der LTE Router leitet die Pakete entweder zum Internet Gateway oder zum internen UxV-VPN Server. Innerhalb des VPN können alle LTE-UEs untereinander paarweise kommunizieren.

Das LTE eNodeB ist mit dem EPC durch die S1 Schnittstelle verbunden. Diese Schnittstelle erlaubt die Anbindung mehrerer eNodeBs zu selben Zeit, beispielsweise um ein Multi-cell Netz aufzuspannen. In den gegebenen Szenarien wird ein eNodeB mit dem EPC verbunden.

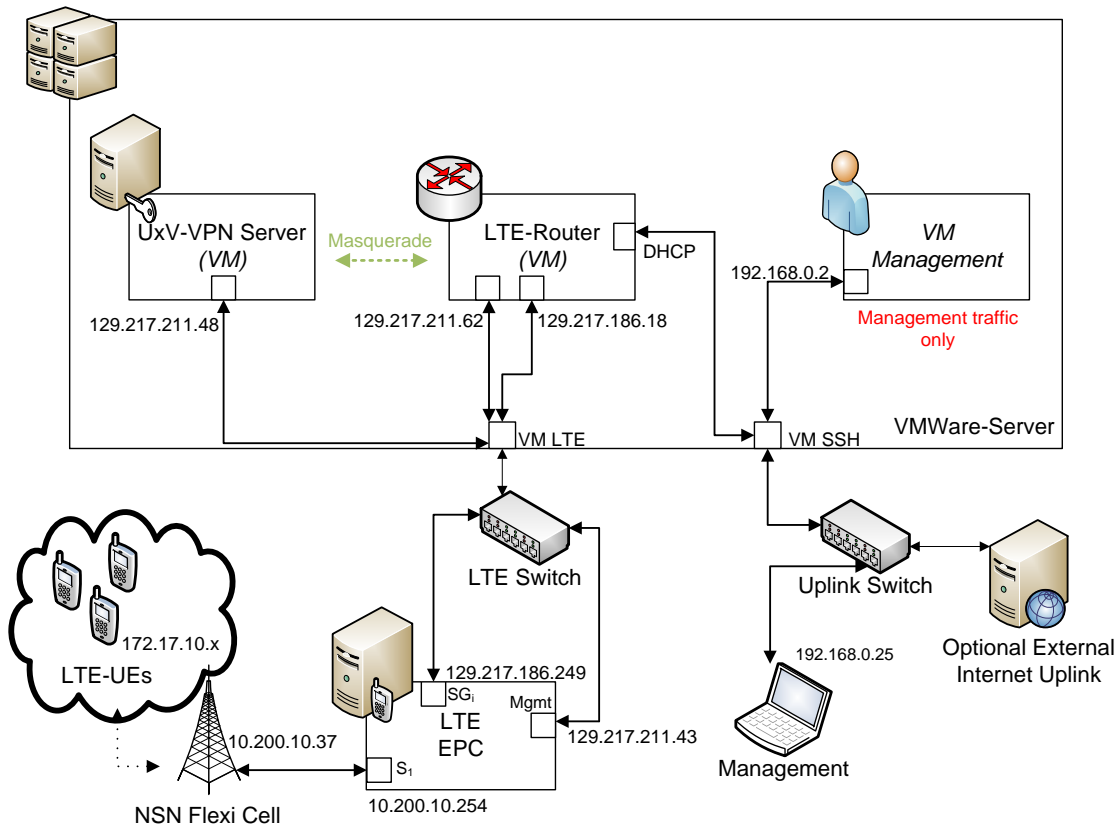


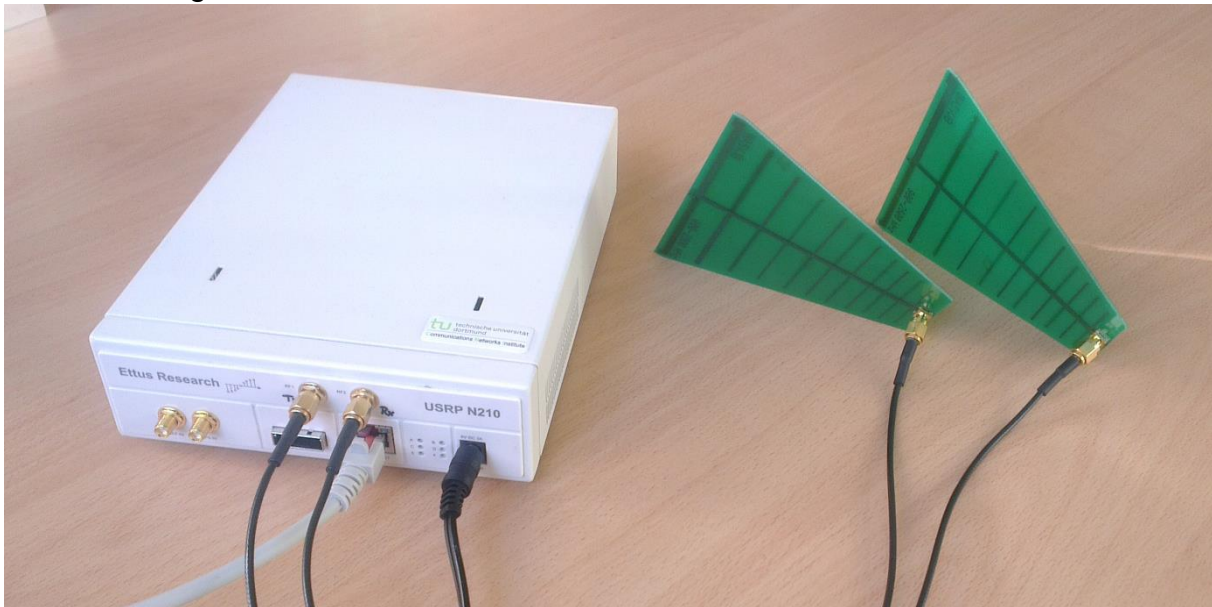
Abbildung 19: Überblick über die LTE Netz Infrastruktur (Quelle: TU Dortmund)

4.3.2 LTE Femto Cells

Für Szenarien wie das in ANCHORS betrachtete, ist die Mobilität wichtig. Daher wird die Verwendung von LTE Femto Zellen als Basisstation evaluiert, Femto Zellen sind deutlich kleiner als herkömmliche Basisstationen. Zu diesen Zweck wird ein USRP N210 von Ettus Research (Abbildung 20) im Zusammenspiel mit einer eNodeB Software von Amarisoft verwendet. Die Femto Zelle wird in gleicher Weise mit dem EPC (durch das S₁ Interface) verbunden wie ein herkömmliches eNodeB. Die Software Defined Radio (SDR) Hardware besteht nur aus der Sendeeinheit inkl. Antennen und einem Computer mit der eNodeB Software.

Die USRP N210 Sendeeinheit kann bei einer Trägerfrequenz von 0 bis 6 GHz mit einer Rate von 50 Mega Samples pro Sekunden im Up- and Downlink betrieben werden. Wegen der hohen Anforderungen an die CPU des Computers um die LTE Frame Struktur, das De- und Encoding etc. kann die eNodeB Software maximal 20 MHz Bandbreite im Down- und Uplink betrieben werden. Die maximale Ausgangsleistung des USRP beträgt 100 mW. Weil LTE Orthogonal Frequency Division Multiple Access (OFDMA) im Download verwendet, wird das Dämpfungsglied mit einer hohen Peak-

to-Average-Power-Ratio (PAPR) belastet wird, begrenzt die eNodeB Software die Sendeleistung.



**Abbildung 20: LTE Femto Cell USRP N210 Radio Frontend mit direktionalen Antennen
(Quelle: TU Dortmund)**

Um den Beschränkungen zu begegnen werden direktionale Antennen verwendet. Dies verursacht in den meisten Krisenmanagementszenarien keine Nachteile, da die Kommunikationsinfrastruktur üblicherweise am Rand der gefährlichen Zone aufgebaut wird.

4.3.3 Leistungsbewertung von LTE Femto Cells

Im nächsten Schritt soll evaluiert werden wie die erreichbare Abdeckung und die Datenrate innerhalb einer gefährlichen Zone aussehen. Zu diesem Zweck werden Daten-Transfer Messungen in verschiedenen Distanzen durchgeführt.

Der Messaufbau besteht aus einem SDR als eNodeB wie zuvor beschrieben. Das SDR operiert mit einer Bandbreite von 20 MHz im 2,6 GHz Frequenzband. Die gerichteten Antennen haben einen Antennengewinn von 5 dBi. Als mobiles Equipment wird ein handelsübliches USB-LTE-Modem (Huawei) an einen Laptop angeschlossen. Dieses Paket wird in unterschiedlichen Distanzen in direkter Sicht (line-of-sight) zu den SDR Antennen aufgebaut. Für den Datentransfer wird die Software „iperf“ in dedizierten Up- und Downlink Tests verwendet.

Die Abbildung 21 zeigt die Ergebnisse dieser Tests. Jeder Wert beschreibt die mittlere Datenrate eines kontinuierlichen ein-minütigen Transfers. Die maximal erreichte Datenrate ist ungefähr 31 Mbit/s im Downlink und 17 Mbit/s im Uplink in einer Distanz von 22m. Die Ergebnisse der geringeren Entfernung von 11,5m weisen niedrigere Datenraten auf, da der Aufbau es in dieser Entfernung nicht erlaubte den Laptop im Ausleuchtungsbereich der Antennen aufzustellen. Die größte Entfernung beträgt 112m

mit einer gemessenen Datenrate von 4 Mbit/s (Downlink) und 0,4 Mbit/s (Uplink). Darüber hinaus erhöht sich die Anzahl der Timeouts, eine Linkstabilität ist nicht mehr gegeben.

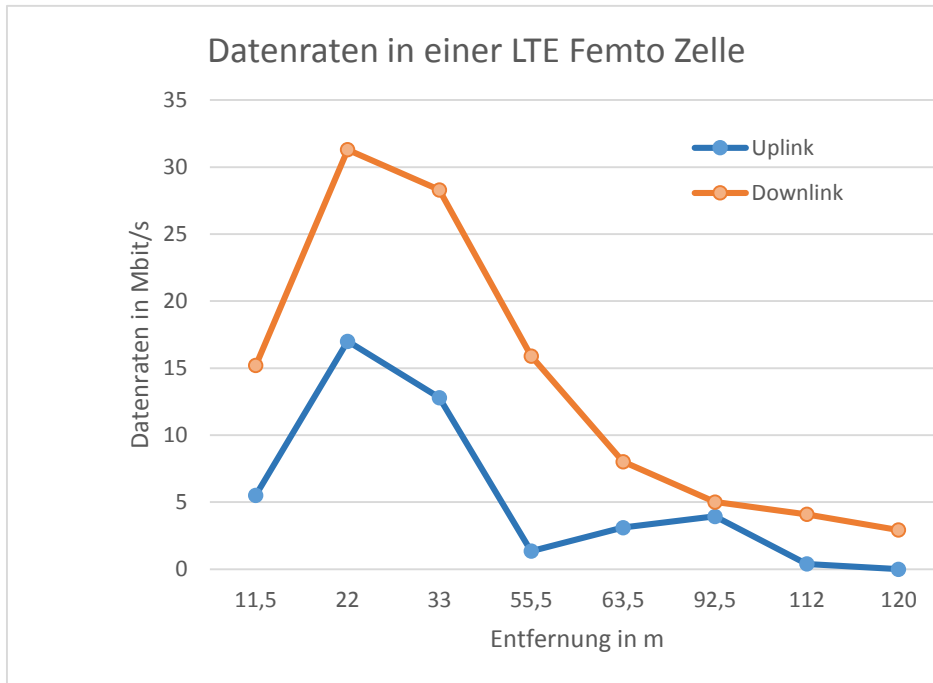


Abbildung 21: Datenrate in einer LTE Femto Zelle mit gerichteten Antennen bei unterschiedlichen Distanzen (Quelle: TU Dortmund)

Um größere Distanzen zu erreichen müsste entweder die Sendeleistung erhöht werden und in Verbindung mit einem empfindlicheren Empfänger oder ein tieferes Frequenzband mit einem geringeren Pfadverlust verwendet werden. Das Letztere wird verworfen aufgrund der regulatorischen Vorgaben in Deutschland, der TU Dortmund verfügt über eine Forschungslizenz ausschließlich im 2,6 Ghz Band.

Die Resultate zeigen, dass eine LTE Femto Zelle als mobiles eNodeB genutzt werden kann. Moderate Modifikationen an der Sendeeinheit und dem Frequenzband erhöhen den Nutzen deutlich. In der Großübung der Feuerwehr wird allerdings eine klassische Basisstation verwendet um eine ausreichende Zellabdeckung und Datenrate zu erhalten.

4.3.4 LTE in der Deutschen Großübung

Während der Großübung der Feuerwehr wurde ein LTE Netz wie in Abbildung 22 zu sehen ist verwendet. Das LTE eNodeB verwendet eine Bandbreite von 20 MHz bei einer Trägerfrequenz von 2650 MHz im Downlink und 2530 MHz im Uplink bei einer Sendeleistung von 8W und einer gerichteten Antenne.

Auf diese Weise konnte während der Durchführung der Übung ein zuverlässigen zweiter Link für die Kommunikation zwischen Robotern und Bodenstation bereitgestellt werden. In dieser Konfiguration zeigten Tests eine Reichweite von mehr als 1,5 km.

Weiter gehende Tests konnten aufgrund der Bodenbeschaffenheit und der Notwendigkeit eines Sicherheitspiloten für die UAVs nicht durchgeführt werden.



Abbildung 22: Installation von LTE EPC und eNodeB in einem Wagen (links) und eine gerichtete Antenne (rechts) mit Fokus auf den Gefahrenbereich während der Großübung der Feuerwehr (Quelle: TU Dortmund)

4.3.5 Optimierung von LTE Netzen durch Smart Traffic Generatoren

Die Nutzung von UAVs und UGVs im Krisenmanagement erfordert sehr robuste Kommunikationsinfrastrukturen um die jederzeitige Steuerung der Roboter zu garantieren. In privat-Anwender orientierten Netzen steht hingegen die wahrgenommene Zufriedenheit der Nutzer im Vordergrund bei Designüberlegungen: der Netzbetreiber optimiert das Netz für hohe Reichweite und höchstmöglichen Datendurchsatz. In diesen Netzen erhalten Endgeräte mit nachteiligen Kanalbedingungen schlechte Applikationsdatenraten und Verbindungsfehler, welche von den Nutzern zumeist hingenommen werden. In Szenarien wie dem in ANCHORS betrachteten, bedeutet eine Verbindungs- oder Dienstfehler hingegen, dass es keine Möglichkeit gibt notwendige Steuerinformationen zum Roboter zu übertragen. Die Konsequenzen dieser Störung können fatal sein, daher ist es unerlässlich die Netze genau hierauf auszurichten. Die Robustheit eines Netzes gegenüber Funkausbreitungseigenschaften, Anomalien im Datentransfer oder technischen Fehlern sowie externen Angriffen muss gegeben sein.

Der Netzbetreiber muss folglich die Zuverlässigkeit und Robustheit seiner Kommunikationsinfrastruktur mit geeigneten Methoden anhand spezifischer Key Performance Indicators (KPIs) validieren. Diese KPIs müssen auf die Anwendung zugeschnitten sein, also an die Anforderungen von ANCHORS angepasst werden, und im gesamten Zellbereich geprüft werden. Dazu werden traditionellerweise Fahrzeuge mit Messequipment ausgestattet, die dann durch den Zellbereich fahren. Das Ziel ist es eine Zuordnung von gemessenen Werten zu einer geografischen Position zu erhalten und somit eine Funkfeldkarte zu erstellen. Diese Vorgehensweise bedeutet

einen hohen Aufwand für die Durchführung der Tests und einer zeitlich beschränkten Aussagekraft der Messwerte.

Um diesem Problem zu begegnen wird eine innovativer Methode vorgestellt, um die räumliche Verteilung der Systemleistung eines mobile Netzes zu evaluieren: Smart Traffic Generators (STGs). Die Abbildung 23 zeigt die Struktur dieses STG Systems.

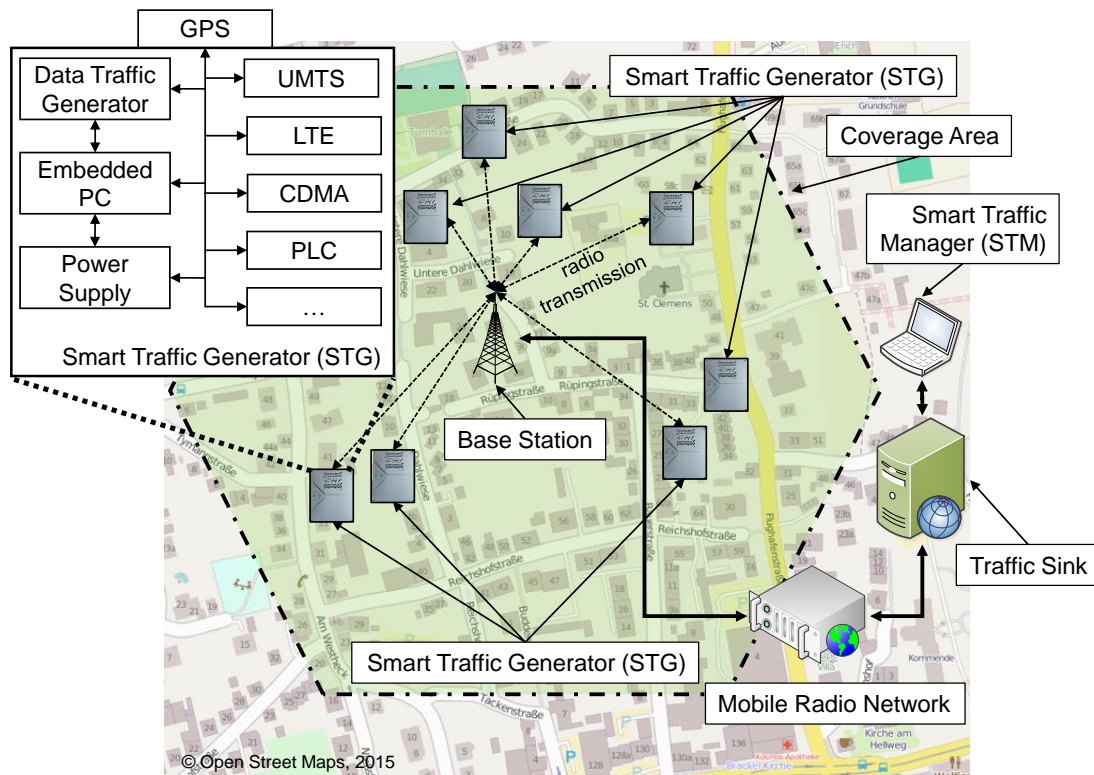


Abbildung 23: Übersicht der Architektur für einen Stresstest einer kritischen Kommunikationsinfrastruktur mit der Nutzung von Smart Traffic Generators [8]

Wie beschrieben ermöglicht das System räumlich-verteilte Verkehrsmuster innerhalb einer Funkzelle zu generieren um das Zellverhalten in kritischen Szenarien durch geeignete Feldtests zu evaluieren. Die STGs ermöglichen die effiziente Durchführung von multiplen Messstudien durch einen Applikationen-Scheduler, welche über eine grafische Oberfläche (Smart Traffic Control Center, STCC) zugänglich ist. Anschließend detektieren integrierte post-processing Methoden Leistungsprobleme und der Netzbetreiber kann das Netz entsprechend optimieren.

Realisierung von QoS in LTE Netzen

In LTE Netzen gibt es mehrere Methoden QoS Anforderungen zu erfüllen.

1) QoS Class Indicators QCI

In der Absicht QoS Anforderungen für eine Vielzahl von Diensten zu erfüllen, bietet LTE eine Lösung in Form von sogenannten QCI an. Neun verschiedenen QCI Klassen

(1-9) geben verschiedene Verkehrsprioritäten und QoS Anforderungen wie eine Guaranteed Bit Rate (GBR) oder die Paketverzögerung an. Für UxV Dienste sind insbesondere eine garantierte minimale Datenrate und eine jederzeitige Verbindung zum mobilen Netz wichtig.

2) Resource Scheduling

Der LTE Scheduler, welcher Teil der eNodeB Implementierung ist, ist verantwortlich für die Zuordnung von Zeit- und Frequenzressourcen in Form von Resource Blocks (RBs) zu den Endgeräten, die Daten senden oder empfangen möchten. Das Ressourcen Scheduling teilt die Ressourcen zu jedem Transmit Time Interval (TTI) von 1 ms zu. Der Scheduling Algorithmus nutzt die Prioritäten, die von den QClis vorgegeben werden. Unter Berücksichtigung des Modulation and Coding Scheme (MCS) beeinflusst die Anzahl der zuordneten Resource Blocks direkt die Datenrate des Endgeräts.

Beschreibung der STG Architektur

In diesem Abschnitt wird das eingeführte STG System vorgestellt. Als erstes wird das generelle Konzept erläutert und anschließend die verschiedenen Teile des Systems näher vorgestellt.

Das STG System erlaubt die Generierung von verschiedenen Testszenarien mit realistischem, Applikationsspezifischem Datenverkehr und führt das Netz systematisch an seine Leistungsgrenzen. Die relevanten Leistungsindikatoren sind in diesem Fall die erreichbare Kapazität und die Netzstabilität unter hoher Last.

- Die Kapazität beschreibt das Verhältnis von erreichbarer Datenrate einer Funkzelle zu einer normalisierten Oberfläche (z.B. Mbit/s pro km²). Eine verwandte Messeinheit ist die spektrale Effizienz (Mbit/s pro Hz).
- Die Stabilität eines Netzes beschreibt das Verhalten in Überlast-Situationen. Das Ziel ist es einen Systemabsturz unter allen Umständen zu vermeiden. Verwendet das System Prioritätsmechanismen, kann weiter geprüft werden ob diese eingehalten werden.

Die Abbildung 23 zeigt die Architektur des STG Systems. Ein Webserver auf jeder STG Einheit ermöglicht den Fernzugriff für die Konfiguration und die Ausführung von Tests. Die STGs produzieren verschiedene Verkehrstypen, wie TCP oder UDP, maximale Verkehrsrate oder räumlich-verteilte Verkehrsmuster. Ein STG kann das Verhalten von einer großen Anzahl von Endgeräten emulieren. Das bedeutet ein STG kann den Verkehr als Mischung verschiedener Applikationsarten wie Webdownload, Voice over Internet Protocol (VoIP) etc. generieren.

Bei der Ausbringung von STGs müssen die spezifischen Bedingungen vor Ort betrachtet werden. Verschiedene Kanalbedingungen die durch unterschiedliche Distanzen, Abschattungseffekte und andere Hindernisse verursacht werden, müssen ausgewogen berücksichtigt werden.

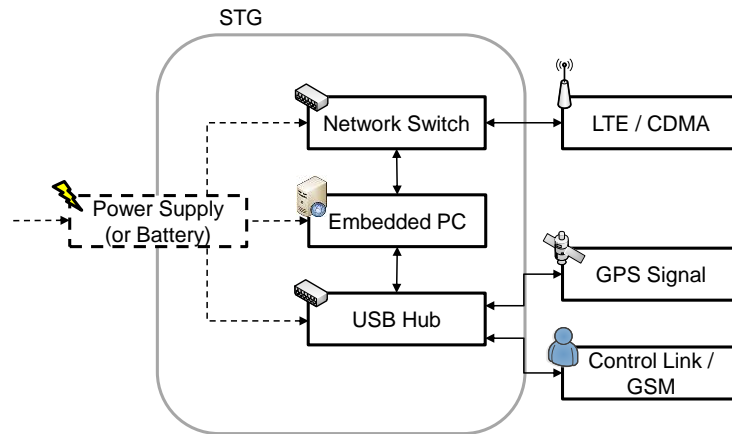


Abbildung 24: Hardware Architektur eines STG [8]

Die Abbildung 24 beschreibt die Hardware Architektur eines STG. Generell besteht jeder STG aus einem Raspberry Pi Embedded PC und Kommunikationsmodulen zur Datenerzeugung und Übermittlung. Es ist möglich verschiedene Kommunikationsmodule (z.B. ein LTE und ein CDMA Modem) in einem STG zu betreiben und via Ethernet oder USB zu verbinden. Für Positionsinformationen und zur hochgenauen Zeitsynchronisierung aller Geräte wird ein GPS Modul verbaut. Zudem gibt es die Möglichkeit einen Akku zu installieren, um vom Stromnetz unabhängig zu sein. Die Abbildung 25 zeigt den Innenraum einer STG Box.

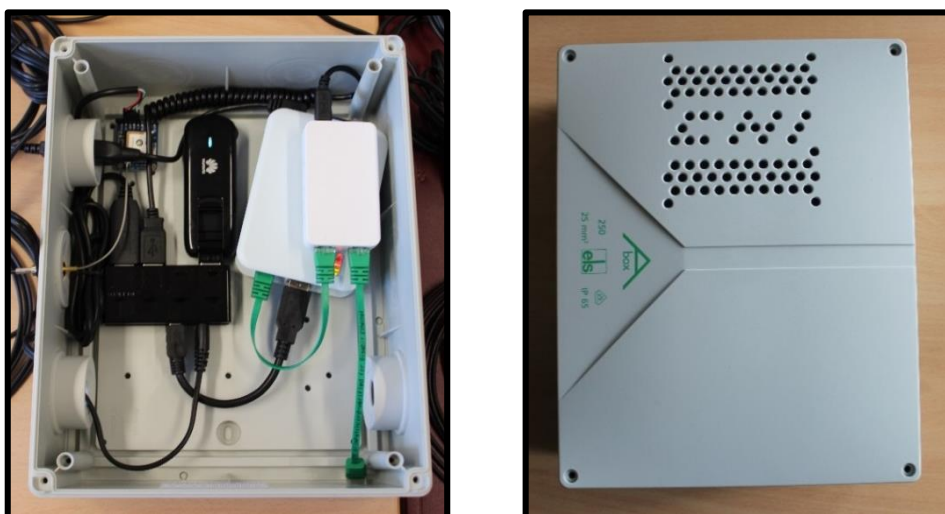


Abbildung 25: Innenleben einer STG Box [8]

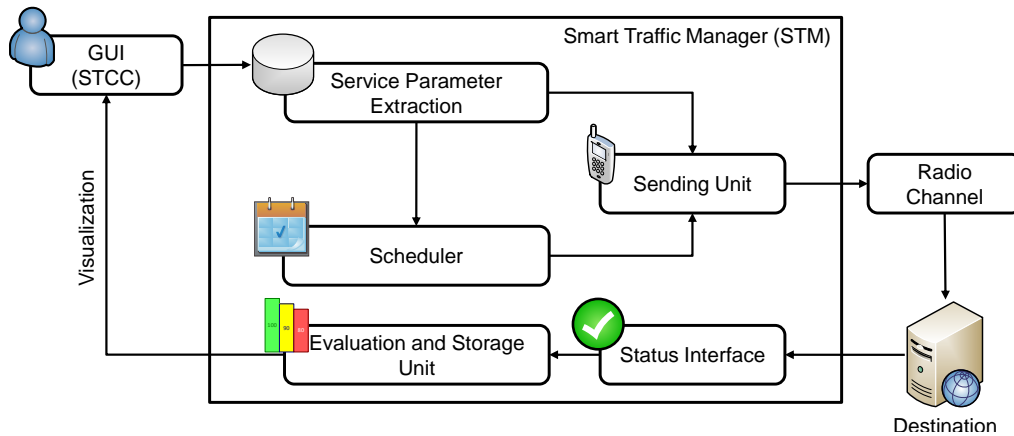


Abbildung 26: Softwarearchitektur der STG [8]

Die Softwarearchitektur wird in Abbildung 26 skizziert. Sie umfasst eine grafische Benutzerschnittstelle (GUI), hier Smart Traffic Control Centre (STCC, vgl. Abbildung 27) genannt. Über das STCC kann der Benutzer die Feldtests initiieren und die verwendeten Verkehrsprofile auswählen. Vorgefertigte Profile, z.B. für TCP und UDP Tests, ergänzen die Auswahl. Ein weiterer Aspekt die direkte Steuerung jedes einzelnen STG.

Nachdem der Benutzer die Verkehrsprofile gewählt hat, entscheidet das STCC welche STG Klienten für die Messung benötigt und transferiert die entsprechenden Daten zum Smart Traffic Manager (STM) des Klienten. Das STM ist die Steuerungseinheit jedes STG. Ein zusätzlicher Scheduler kann eine Sende-Queue organisieren um einen Zeitbezogenen Prozess zu realisieren. Im STM werden alle Messdaten gesammelt und erste statistische Auswertungen vorgenommen. Die Sending Unit generiert die Datenpaket und initiiert den Sendevorgang. Die Evaluation and Storage Unit transferiert die Messresultate kontinuierlich zum STCC.

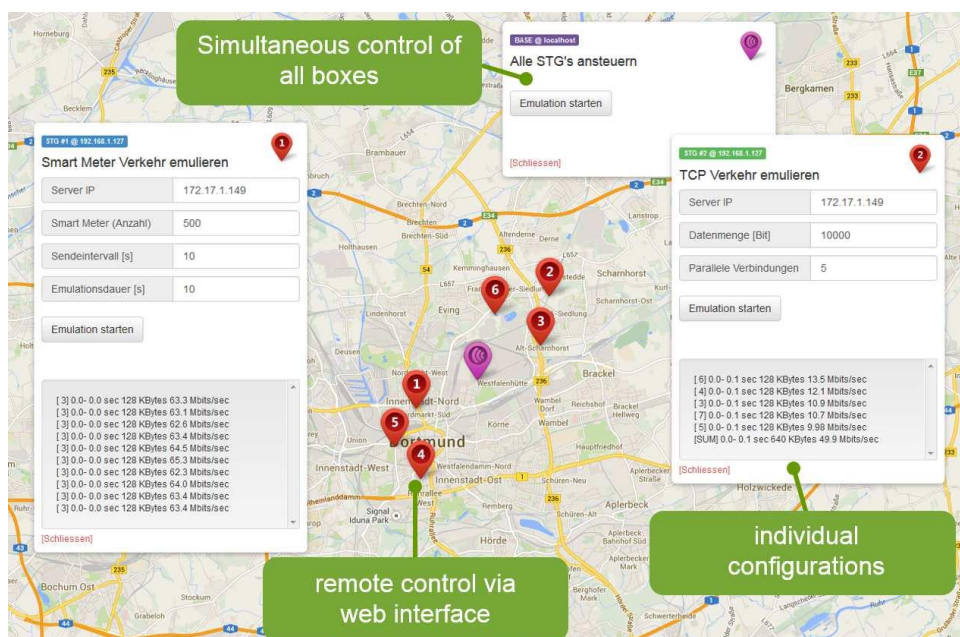


Abbildung 27: Grafische Benutzerschnittstelle (STCC) [8]

Ergebnisse der Feldtests: Leistungsfähigkeit von LTE für Applikationen mit zeitkritischen Anforderungen

Im Folgenden werden die Ergebnisse einer Messkampagne vorgestellt, um die Vorteile des STG Systems im Vergleich zu traditionellen Fahrttests herauszustellen. Das Ziel der Studie ist die Analyse der Eignung des LTE Netzes für die Übertragung von Steuerungsverkehr in UxV-Netzen. Zusätzlich sollen die Feldtests Möglichkeiten der Optimierung eines Netzes für ebensolchen Datenverkehr bei einer räumlich verteilten Verkehrslast aufzeigen. Zu diesem Zweck werden sieben STGs in Reichweite einer dedizierten LTE Zelle installiert. Die Orte weisen verschiedene Funkcharakteristiken auf. Der Reference Signal Received Power (RSRP) Wert gibt eine Einordnung wieder. Ein hoher RSRP bedeutet gute Kanaleigenschaften, was wiederum in einer hohen Wahrscheinlichkeit für hohe Datenrate mündet. Ein niedriger RSRP weist auf schwierige Kanaleigenschaften und somit geringere Datenraten hin. Die Tabelle 1 zeigt die gemessenen RSRP Werte für jeden STG. STG#001, STG#002 und STG#004 – STG#007 haben gute (-30 to -100 dBm) bis moderate (-100 to -110 dBm) Kanaleigenschaften, wohingegen sich STG#003 am Zellrand in einer schwierigen Umgebung befindet, was in einem RSRP von -119 dBm resultiert, nur knapp oberhalb der Empfängersensitivität von ≈ -120 dBm.

Tabelle 1: Gemessene RSRP Werte für jeden STG [8]

STG Nummer	RSRP [dBm]	Klassifikation der Kanaleigenschaften
STG#001	-78	Gut
STG#002	-100	Moderat
STG#003	-119	Schlecht
STG#004	-82	Gut
STG#005	-50	Gut
STG#006	-77	Gut
STG#007	-80	Gut

Jeder STG transferiert den Datenverkehr im Uplink mit der maximalen Datenrate und evaluiert im Nachgang die tatsächlich erreicht Datenrate. Die Kampagne besteht aus zwei Messungen: 1) Nur ein STG transferiert Daten zur gleichen Zeit. 2) Alle STG übertragen simultan. Dies führt zur geplanten Stresssituation weil der Scheduler der LTE Zelle nun die zur Verfügung stehenden Ressourcen optimal aufteilen muss. Die Tabelle 2 listet alle relevanten Zell- und Datenparameter auf.

Tabelle 2: Konfigurationsparameter der Messkampagnen [8]

Cell frequency	2.6 GHz
Cell bandwidth	20 MHz
Cell duplex mode	FDD
Cell transmission power P_{Tx}	8 W
Antenna Gain of base station G_{BS}	7 dBi
Number of cell sectors N	1
Number of Repetitions per measurement	30
Data packet size D	100 Mbyte
Number of active STGs	1..7
Antenna Gain of STGs G_{STG}	≈ 0 dBi
Used QCI configuration 1	STG#001 to #007: QCI 9
Used QCI configuration 2	STG#001, #002, #004 to #007: QCI 9 STG#003: QCI 5

In den generierten Stresssituationen und wenn die Zelle die Standardkonfiguration nutzt, dann favorisiert der MT Scheduler STGs mit guten Kanalbedingungen in der Absicht den Zelldurchsatz zu optimieren. Dies führt zu der Situation, dass STGs mit schlechten Kanalbedingungen (z.B. am Zellrand) eine kleinere Anzahl von Ressourcen zugewiesen bekommen und somit keine hohen Datenraten erreichen können, insbesondere wenn ein robustes MCS ausgewählt wurde. In Folge dessen sind STGs mit schlechten Kanalbedingungen nicht in der Lage kritische UxV Anwendungen zufriedenstellend auszuführen. Eine mögliche Gegenmaßnahme ist die Verwendung von QCI-Klassen. Der Netzbetreiber hat die Möglichkeit STGs mit schlechten Kanalbedingungen eine höhere Priorität zuzuweisen, wodurch diese mehr Ressourcen erhalten.

Um dieses Problem eingehender zu analysieren, werden Messkampagnen mit folgenden zwei Konfigurationen durchgeführt: In der ersten Konfiguration bekommen alle STGs die gleiche QCI-Klasse 9 zugewiesen. In der zweiten Konfiguration bekommt der STG#003 die höhere QCI-Klasse 5 zugewiesen.

Konfiguration 1: Alle STGs haben die gleiche Priorität

Die Abbildung 28 zeigt die Resultate für die erste Konfiguration als Boxplot mit einem Konfidenzlevel von 95%. In der ersten Messung (grau unterlegt), wo jeweils ein STG sendet, erreichen die STGs mit guten Kanalbedingungen eine durchschnittliche Datenrate von ungefähr 42 Mbit/s. Der STG#002 mit moderaten Kanalbedingungen

erreicht aufgrund eines robusteren MCS eine reduzierte Datenrate von 35 Mbit/s. Am Zellrand erreicht der STG#003 eine Datenrate von 8,7 Mbit/s.

In der zweiten Messung (schwarz hinterlegt) starten alle STGs ihre Transmission zur gleichen Zeit. Das bedeutet, dass der Scheduler nun die Ressourcen verteilen muss. Das zuvor beschriebene Muster bestätigt sich hier, STG#003 bekommt die wenigsten Ressourcen zugewiesen und erreicht eine durchschnittliche Datenrate von 0,4 Mbit/s. Zudem sind viele temporäre Verbindungsverluste festzustellen. Die anderen STGs erreichen dagegen im Mittel eine Datenrate von 6,4 Mbit/s. Dies ist ausreichend für die meisten UxV Anwendungen.

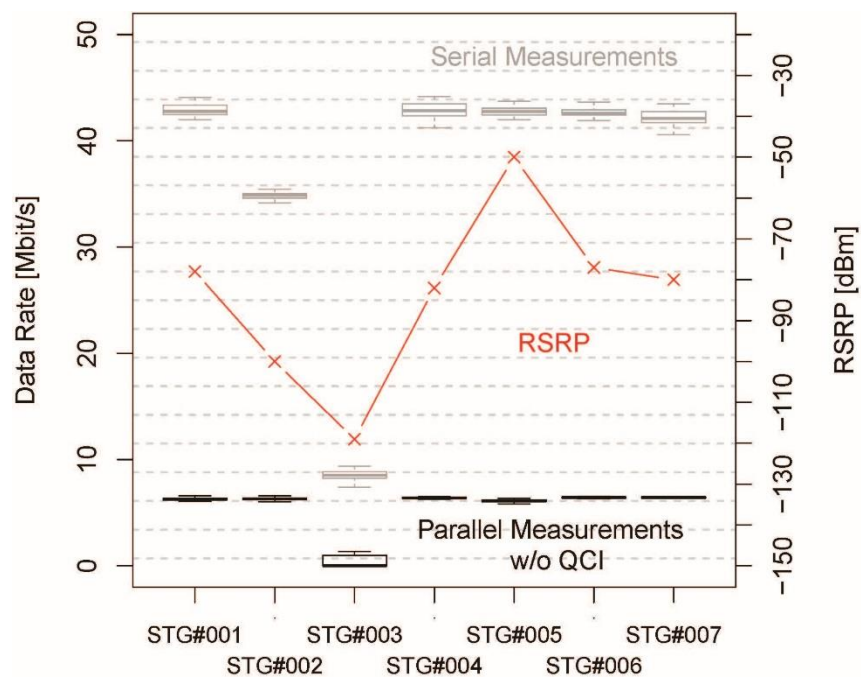


Abbildung 28: Datenraten in Uplink-Richtung ohne QCI-Einfluss [8]

Konfiguration 2: Zuweisung der höheren Priorität an STG#003

Um das Problem der ersten Konfiguration zu beheben, wird nun STG#003 die höhere Priorität (QCI-Klasse 5) zugewiesen. Damit sollte STG#003 mehr Funkressourcen zugeteilt bekommen. Anschließend werden beide Messvorgänge erneut durchgeführt. Die Abbildung 29 zeigt die Ergebnisse dieser Messungen. Wenn alle STGs zur gleichen Zeit übertragen erreicht STG#003 die höchste mittlere Datenrate von 5,7 Mbit/s. Da hierfür der Bedarf an Funkressourcen hoch ist, sinkt die Datenrate für die übrigen STGs ab. Sie erreichen nun eine Datenrate von 2,2 Mbit/s (gute Kanalbedingungen) und 2 Mbit/s (moderate Kanalbedingungen).

Trotz dieser Reduzierung können nun alle STGs stabil kommunizieren mit einer Mindestdatenrate von 1,99 Mbit/s. Das bedeutet, dass in dieser LTE Zelle eine robuste Kommunikationsumgebung für den Einsatz von UxVs gegeben ist.

Die relative hohe Varianz der Ergebnisse (ungefähr 2 Mbit/s) ist auf die dynamische Funkkanalbedingung für STG#003 zurückzuführen. Je nach aktueller Situation müssen diesem STG mehr oder weniger Ressource blocks zugewiesen werden, was ebenso in veränderten Datenraten für die anderen STGs mündet.

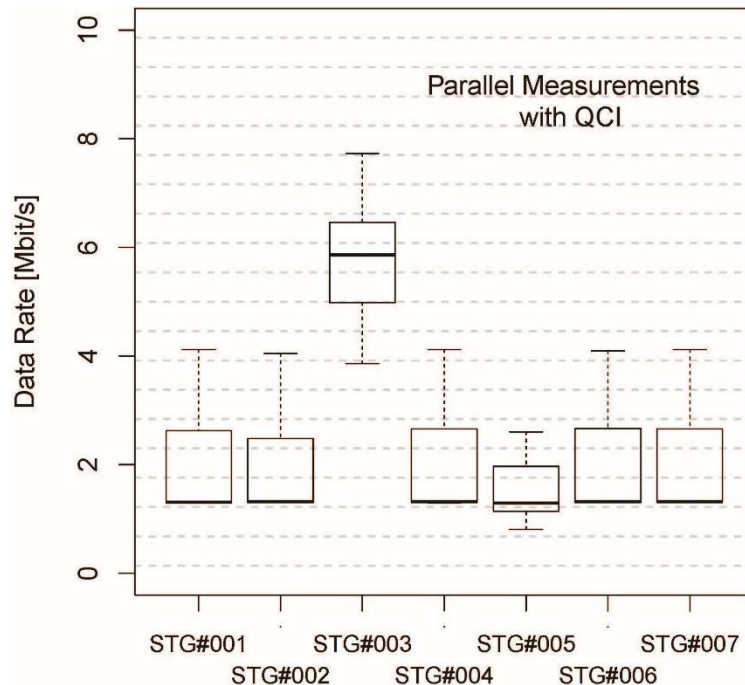


Abbildung 29: Datenraten im Uplink mit QCI [8]

Diese Studie zeigt, dass das vorgeschlagene STG System eine gute Wahl ist um das Systemverhalten zu quantifizieren. Der erweiterte Einsatzbereich im Vergleich zu konventionellen Messungen im fahrenden Auto erschließt eine ganze Reihe neuer Testmöglichkeiten wie dem Stresstest mit vielen gleichzeitig sendenden Entitäten. Zudem lässt sich in der Konfiguration die zeitliche Varianz der Messungen besser untersuchen.

4.4 Ad-hoc Multi-hop Kommunikation

Neben dem Zellularfunksystem LTE wird in ANCHORS noch eine weitere Kommunikationstechnologie eingesetzt: Wireless Mesh Networks.

IEEE 802.11 ist ein Set von Standards um Wireless Local Area Networks (WLAN) zu implementieren. Die Kommunikation findet im 2,4 GHz, 3,6 GHz und 5 GHz Frequenzspektrum statt.

Die gängigsten Standards sind:

- IEEE 802.11a
- IEEE 802.11b

- IEEE 802.11g
- IEEE 802.11n
- IEEE 802.11s

4.4.1 Mesh System Design für unbemannte Roboter

Das Design-Prinzip der vier erstgenannten Standards ist ein zentralisiertes System. Wohingegen der neue IEEE 802.11s Standard die Etablierung eines Mesh-Netzes vorsieht. Die Abbildung 30 zeigt das Mesh-Netz von ANCHORS, das verwendet wird um alle Entitäten miteinander zu vernetzen. Im Vergleich zu zentralisierten Verfahren erhöht die Mesh-Architektur die Robustheit der Kommunikation durch den Einsatz der Multihop-Technologie.

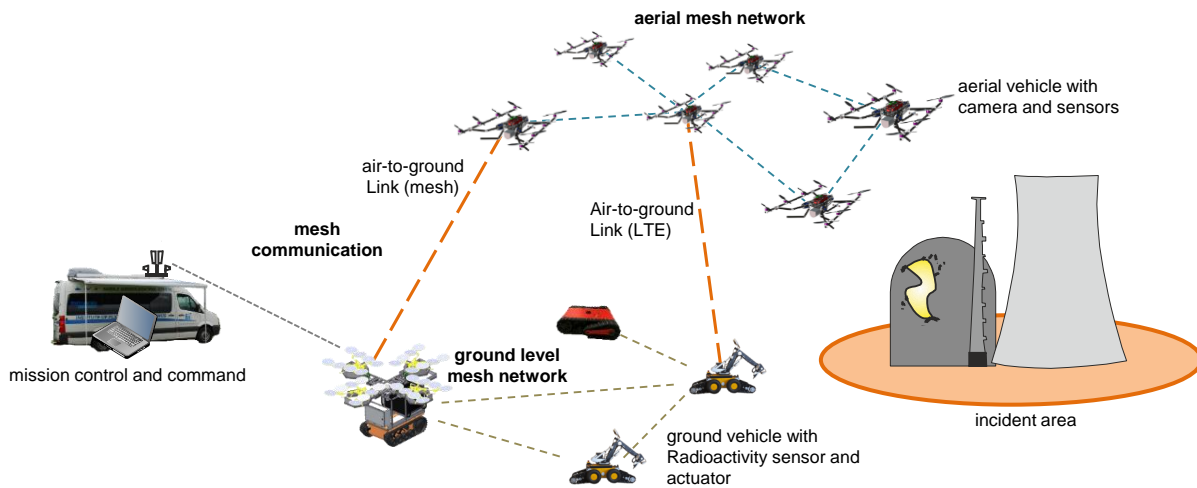


Abbildung 30: Mesh Communication System in ANCHORS (Quelle: TU Dortmund)

Tabelle 3: Überblick über die verwendete WLAN Technologie (Quelle: TU Dortmund)

2,4 GHz Mesh Network	
Verkehrstyp	Command &Control, Payload
Standards/Protokolle	IEEE 802.11n, IEEE 802.11s
Frequenz	2412MHz – 2484MHz
Bandbreite	20MHz / 40MHz
Sendeleistung	20 dBm
Datenraten	Abhängig von Modulation und guard interval: 6.5Mbit/s – 600Mbit/s
Modulation	DSSS / OFDM (BPSK, QPSK or QAM)
Reichweite	Bis zu 450m pro Hop (unter besten Bedingungen)

5 GHz Mesh Network	
Verkehrstyp	Command &Control, Payload
Standards/Protokolle	IEEE 802.11n, IEEE 802.11s
Frequenz	5470MHz – 5725MHz, Channels 100 - 140
Bandbreite	20MHz / 40MHz
Sendeleistung	Bis zu 30 dBm
Datenraten	Abhängig von Modulation und guard interval: 6.5Mbit/s – 600Mbit/s
Modulation	OFDM (BPSK, QPSK or QAM)
Reichweite	Bis zu 200m (bei 20 dBm Sendeleistung)

Bemerkung: Die deutsche Umsetzung der EU Richtlinie 2005/513/EC erfordern den Einsatz von Dynamic Frequency Selection (DFS) und Transmit Power Control (TPC) im Bereich von 5250–5350MHz und 5470–5725MHz. Der Frequenzbereich von 5150–5350 MHz darf nur im Indoor-Einsatz verwendet werden. Nur der Frequenzbereich von 5470-5725 MHz ist für den Einsatz im Innen- wie Außenbereich zulässig.

4.4.2 Test der maximalen Kommunikationsreichweite

Um den Einsatz von WLAN Mesh im UAV-Kontext zu evaluieren wurden verschiedene Testszenarien durchgeführt.

Eine erste wichtige Frage die es zu beantworten gibt ist die maximale Reichweite der direkten Verbindung im Netz. Die Abbildung 31 zeigt die Ergebnisse³ einer Messung im Freifeld. Dabei wurden zwei UAVs genutzt, diese waren zunächst 10m voneinander entfernt. Im Flug wurde die Distanz kontinuierlich erhöht. Bei einer Entfernung von ungefähr 450m wurde die Empfangssignalleistung (RSS) zu gering für eine ausreichend gute Kommunikation.

³ N. Goddemeier, C. Wietfeld, "Investigation of Air-to-Air Channel Characteristics and a UAV Specific Extension to the Rice Model", In IEEE GLOBECOM 2015 Workshop on Wireless Networking, Control and Positioning of Unmanned Autonomous Vehicles (Wi-UAV), San Diego, USA, Dezember 2015

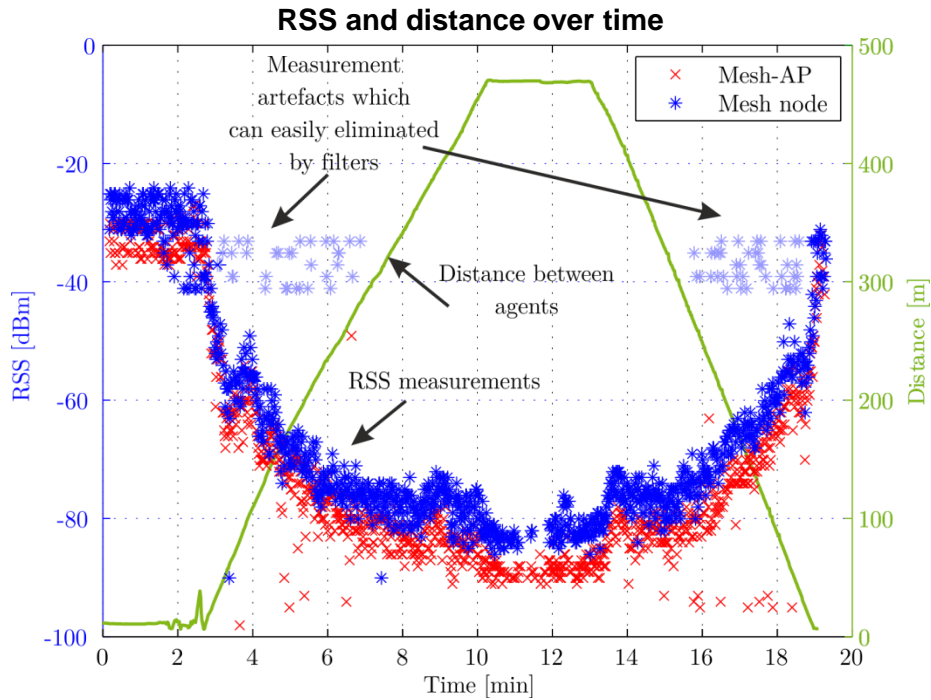


Abbildung 31: Analyse der maximalen Reichweite der Kommunikation für einen Hop (Quelle: TU Dortmund)

4.4.3 Messung des Einflusses der Antennenausrichtung

Als nächstes wurde die Antennencharakteristik und deren Einfluss auf den Kanal mithilfe eines UAVs und einer stationären Bodenstation getestet. Das UAV flog dabei ungefähr 100m von der Bodenstation weg und befand sich in einer Höhe von 25m. Das UAV rotierte in dieser Position um die eigene Z-Achse. Die Antennen sind auf dem

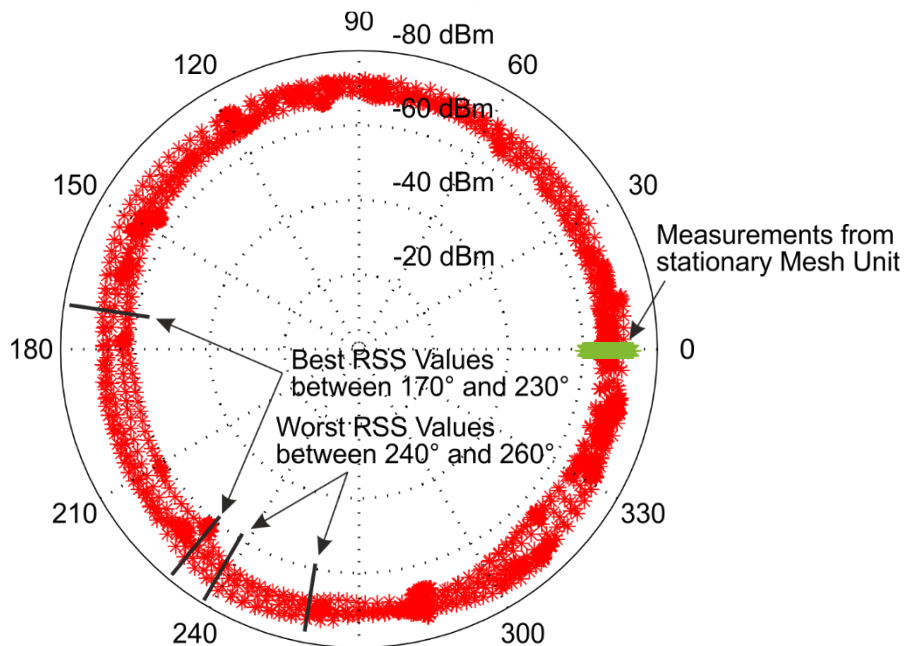


Abbildung 32: Einfluss der Antennenausrichtung (Quelle: TU Dortmund)

UAV in verschiedenen Ausrichtungen befestigt. Die gemessene Empfangssignalstärke (RSS) ist in einem Bereich von $[-78 \text{ dBm}; -60 \text{ dBm}]$ (vgl. Abbildung 32) und dabei gleichverteilt. Der Effekt der Antennencharakteristik beträgt dabei bis zu 10 dBm . Es gibt folglich einen eindeutigen Einfluss der Antennenausrichtung. Dieser könnte beispielsweise durch die Nutzung eines Antennen Trackings an der Bodenstation vermindert werden.

5. AP 5 – Cooperative Swarm Behavior

Der Fokus von Arbeitspaket 5 ist die Entwicklung des kooperativen Schwarmverhaltens für verteilte Messungsstrategien mit heterogenen Robotersystemem. Auf Basis der Vorarbeiten⁴⁵ wurde das kooperative Schwarmverhalten für den ANCHORS Anwendungsfall erweitert. Als erster Schritt wurde eine projektspezifische Systemarchitektur designet, mit der die Ausführung verschiedener Schwarmalgorithmen ermöglicht werden sollte. Das Swarm Command System ist dabei die zentrale Einheit eines Agenten. Im zweiten Jahr lag der Fokus auf der Verbesserung der Robustheit des Kommunikationssystems und der Integration der Bodenroboter in das Gesamtsystem. Im dritten Jahr wurde die Architektur finalisiert und alle Komponenten integriert.

5.1 Architektur der Schwarmsubsysteme

Die Hauptaufgabe des Schwarmsubsystems ist die Steuerung des Verhaltens aller Roboter. Diese Komponente interagiert folglich mit allen anderen Komponenten des UAV Systems wie der lokalen Fluglagenregelung, den Payload-Diensten und dem Kommunikationssystem.

Der *Swarm Command Service* ist die zentrale Komponente eines Agenten. Deren Hauptaufgabe ist die Koordination aller Subkomponenten des *Cooperative Swarm Behavior System* und die Steuerung des Informationsaustauschs zu den anderen Komponenten des UAV Systems.

⁴ N. Goddemeier, K. Daniel, C. Wietfeld, "Role-Based Connectivity Management with Realistic Air-to-Ground Channels for Cooperative UAVs", In *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 30, no. 5, pp. 951-963, Juni 2012.

⁵ N. Goddemeier, S. Rohde, C. Wietfeld, "Experimental Performance Evaluation of Role-Based Connectivity Management for Cooperating UAVs", In *79th IEEE Vehicular Technology Conference (VTC)*, Mai 2014.

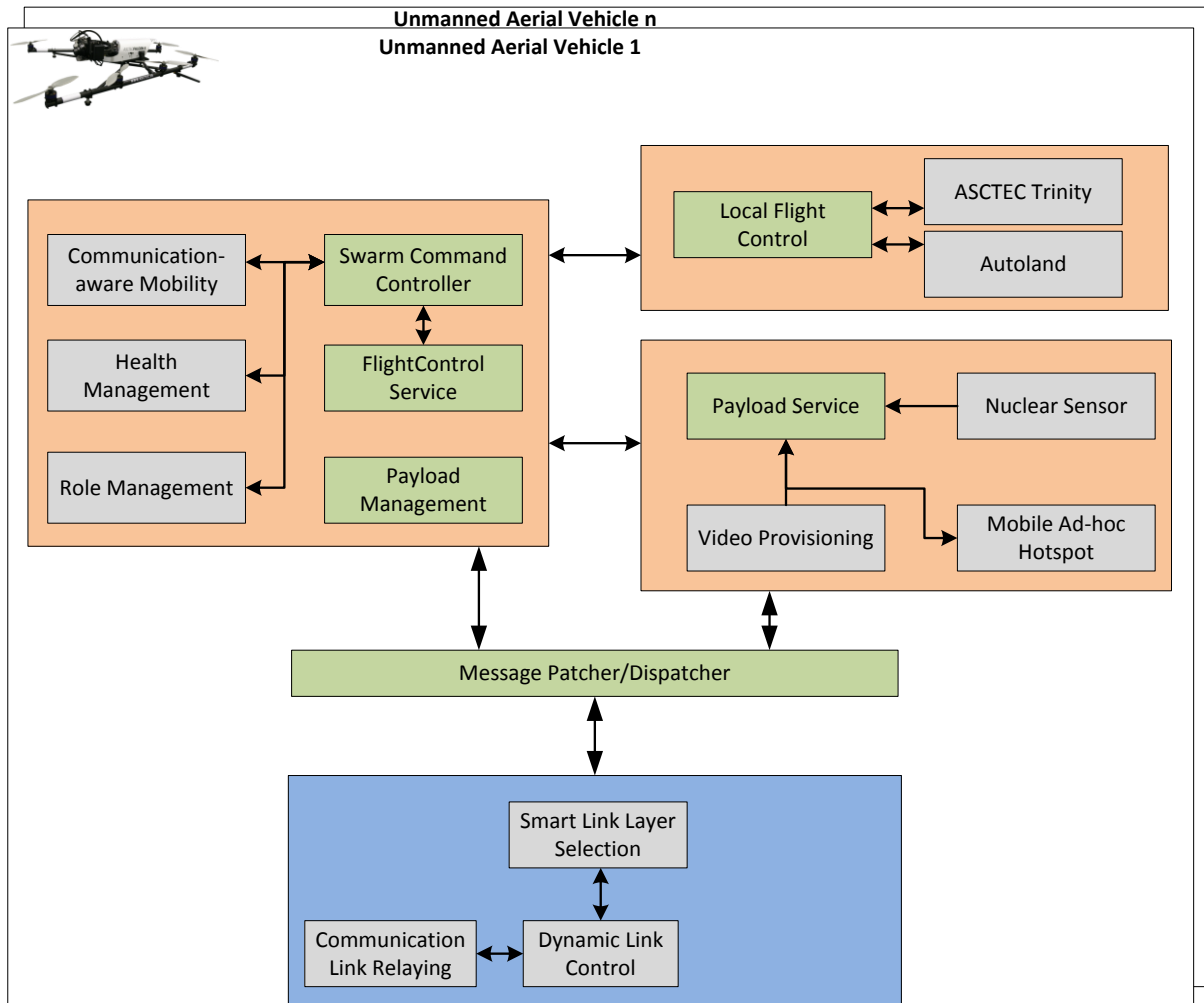


Abbildung 33: Finale Architektur des UAV Systems (Quelle: TU Dortmund)

Die folgenden Komponenten bilden die Basis des Schwarmsubsystems:

- **Swarm Command Controller**

Der *Swarm Command Controller* ist der Direktor des Schwarmsystems. Er koordiniert die Interaktion mit allen anderen Teilen des Systems und steuert auch alle angeschlossenen Subkomponenten.

- **Health Management**

Das *Health Management* überwacht den Status des gesamten Systems. Wenn eine Komponente einen kritischen Fehler meldet, muss entschieden werden ob eine sofortige Reaktion erforderlich ist. Im Fall eines niedrigen Akku-Ladestands kann das Health Management den Rückflug zur Ladestation veranlassen. Anweisungen des Health Management erhalten die höchste Priorität während des Einsatzes.

- **Role Management**

Das *Role Management* bestimmt die generellen Handlungsrichtlinien des Agenten. Es beachtet die aktuelle Kommunikationsumgebung und Erkundungsaspekte und aggregiert daraus die "Rolle", welche der Agent

erfüllen soll. Jede Rolle aktiviert dabei ein festgelegtes Set an Mobilitätsverhalten.

- **Communication-aware Mobility**

Die aktivierten Mobilitätsalgorithmen und der aktuelle Status von Kommunikation, Exploration und Status des Agenten bilden die Grundlage für die Festlegung der Bewegung des Agenten. Diese Komponente integriert und steuert alle implementierten Verhalten.

- **Swarm Navigation Service**

Der *Swarm Navigation Service* transformiert die Resultate der Communication-aware Mobility in eine Liste von Wegpunkten. Diese Wegpunkte werden zum Motion oder Flight Control Service übertragen.

- **Flight Control Service**

Dieser Dienst interagiert mit der lokalen Bewegungsregelung des Roboters, daher wird dieser Dienst jeweils an die speziellen Roboter wie UAVs, UGVs und das MTS angepasst.

- **Payload Management**

Diese Management Komponente integriert verschiedene Arten von Payload in das Schwarmsubsystem. In ANCHORS ist dies insbesondere der Radioaktivitätssensor.

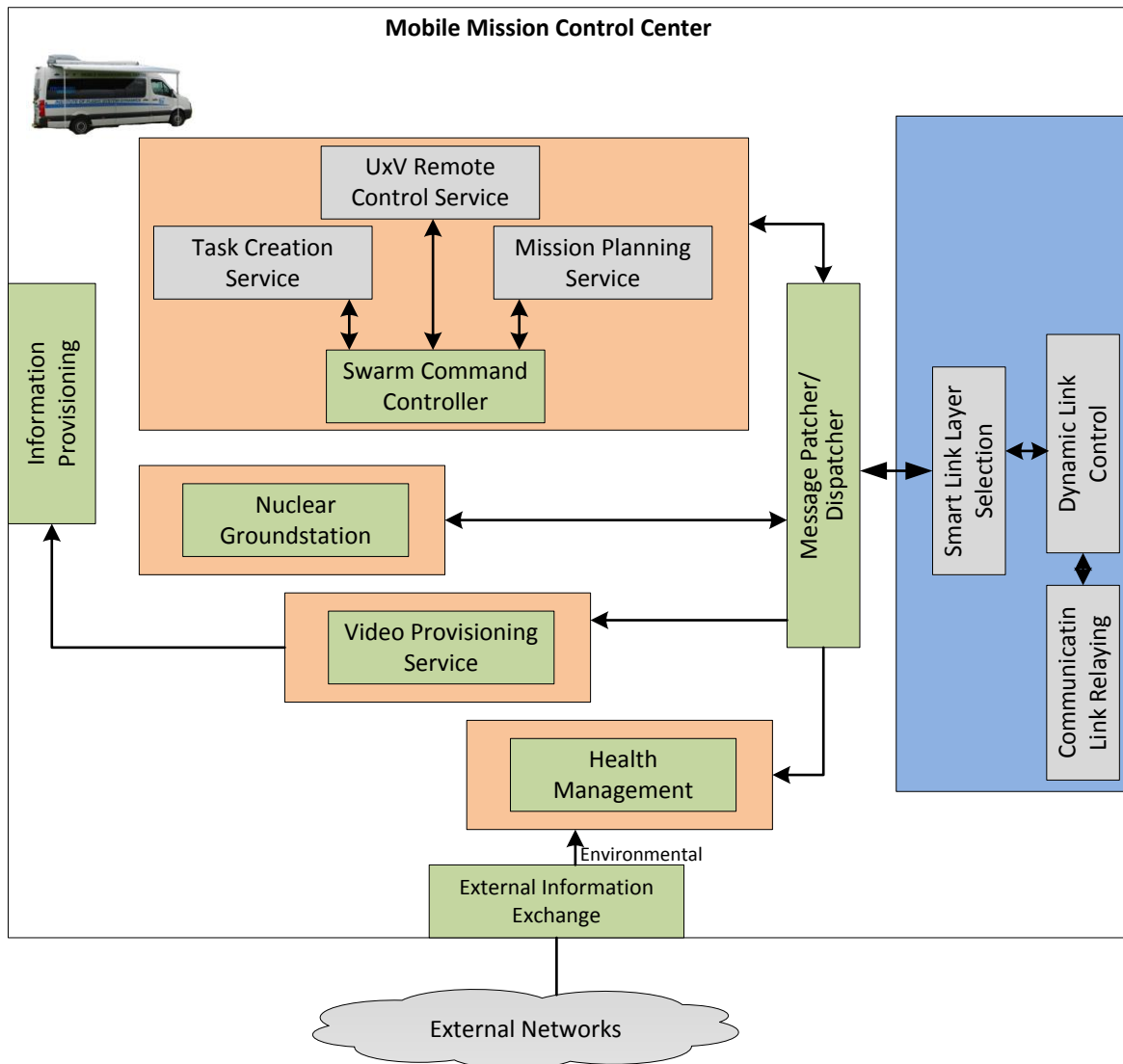


Abbildung 34: Finale Architektur der MMCC Softwarekomponente (Quelle: TU Dortmund)

Das Gegenstück des Roboter-Schwarmsubsystems ist die Bodenkomponente des Schwarmsystems (vgl. Abbildung 34). Durch die Agenten-basierte Struktur des Schwarmsystems wird motiviert, dass die MMCC Komponente nicht die Wegpunktnavigation selbst durchführt, aber bei der Missionsplanung und Task-Erstellung unterstützt.

Die folgenden Komponenten sind Teil des MMCC Schwarmsystems:

- **Swarm Command Controller**
Vergleichbar zum UAV System ist der *Swarm Command Controller* der Dirigent des Systems. Es ist einerseits die Schnittstelle zu den Robotern und andererseits ebenso die Schnittstelle zu dem Operator.
- **Task Creation Service**
Die generelle Mission ist Grundlage für die Bestimmung von Tasks auf einem abstrakten Level, wie z.B. eine nukleare Erkundungsmission. Konkrete

Wegpunkte werden abgeleitet und an das UAV übertragen, die Navigation selbst wird allerdings vom UAV Schwarmsubsystem durchgeführt.

- **Mission Planning Service**

Dieser Dienst benutzt Parameter wie die Größe des Missionsgebiets, den Abstand zwischen Suchabschnitten und deren Winkel um eine nukleare Erkundungsmission zu planen (vgl. Abbildung 35).

- **UxV Remote Control Service**

In einigen Fällen wünscht der Anwender die direkte Kontrolle über einen Roboter. Um auch in diesem Fall von den implementierten Sicherheitsprozeduren zu profitieren ist die direkte Steuerung auch Teil des Schwarmsubsystems.

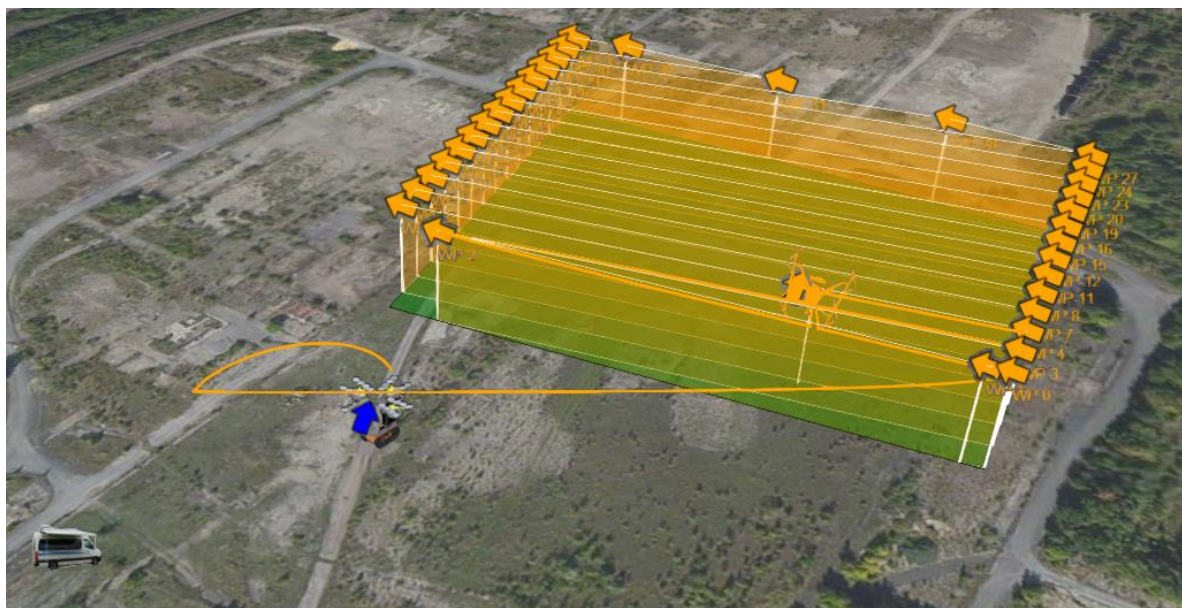


Abbildung 35: Nukleare Erkundungsmission (Quelle: TU Dortmund)

5.2 Spezifikation der Agenten-basierten Schwarmalgorithmen

Anforderungen an Schwarmalgorithmen

Die Kommunikationsaspekte eines Schwarmbasierten UAV Systems für Überwachung und Beobachtung sind in jüngster Zeit vermehrt in den Fokus der Forschung gerückt. Die neuartigen Algorithmen des ANCHORS Systems adressieren die spezifischen Herausforderungen von unvorhergesehenen Ereignissen wie Unfällen mit radioaktivem Material. Daher ist der Fokus die Erkundung der Randschichten einer gefährlichen Wolke während zeitgleich die Kommunikation innerhalb des UAV Schwarms erhalten bleibt. Aufbauend auf existierenden Algorithmen zur Erkundung eines Raums werden zwei Algorithmen vorgestellt, welche die unterschiedlichen Anforderungen optimal

erfüllen sollen: Aerosol-detecting Cooperative Repelling Walk (ADCRW) und Distributed Dispersion Detection (DDD).

5.2.1 Spezifikation der Algorithmen

Aerosol-detecting Cooperative Repelling Walk

Der in vorherigen Arbeiten vorgestellte *Cooperative Repelling Walk (CRW)*⁶ betrachtet die Erkundung eines gesamten Raums. Jedoch ist hier der Fokus auf Teilen des Gesamtraums. Folglich ist der Algorithmus um Möglichkeiten der Schadstofferkennung und Auswertung erweitert. Wenn ein UAV ein neues Zielgebiet auswählen soll, werden alle Nachbarzellen in Betracht gezogen. Für jeden Nachbarn wird ein Wahrscheinlichkeitskoeffizient bestimmt. Dieses zufällige Zellgewicht für den *Cooperative Repelling Walk* $c_w(cell_s, t)$ ist definiert durch

$$c_w(cells, t) = \begin{cases} \mathcal{U}(0,1) + 1 & cell\ unvisited \wedge RSSI_{est.}(cell_s) \text{ suff.} \\ -1 & else \end{cases}$$

wobei $\mathcal{U}(0,1)$ eine gleichverteilte Zufallsvariable mit einem Wert zwischen 0 und 1 ist. Als Erweiterung wird nun zusätzlich die bereits bekannte oder prognostizierte Schadstoffkonzentration bei den Nachbarnoten berücksichtigt:

$$c_w(cells, t) = \begin{cases} \mathcal{U}(0,1) + 1 + \frac{1}{g(cell_s)} & cell\ unvisited \wedge RSSI_{est.}(cell_s) \text{ suff.} \\ -1 & else \end{cases}$$

Dabei ist $g(cell_s)$ die Schadstoffkonzentration in der Nachbarzelle s . Zum Schluss wird der Nachbar mit dem höchsten Koeffizienten als nächstes Ziel ausgewählt. Die Abbildung 36 zeigt die Zielbestimmung für ein UAV. Die weißen Zellen sind nicht erkundet. Die bevorzugten Zellen sind die Randschichten der Wolke, die noch unbesucht sind. Die Wahrscheinlichkeit die erste Zelle zu wählen ist höher, da die Schadstoffkonzentration an der Grenzschicht zurückgehen wird.

⁶ D. Behnke, K. Daniel, and C. Wietfeld, "Comparison of Distributed Ad-hoc Network Planning Algorithms for Autonomous Flying Robots," in: *IEEE Global Telecommunications Conference (GLOBECOM 2011)*, December 2011.

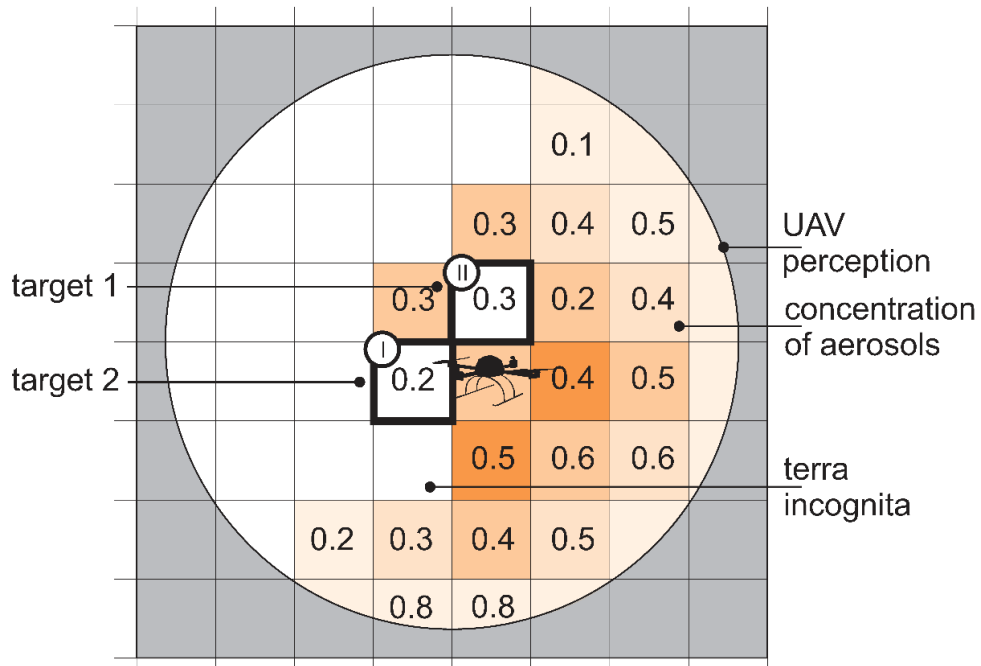


Abbildung 36: Aerosol-detecting Cooperative Repelling Walk [2]

Distributed Dispersion Detection Algorithm (DDD)

Ein Charakteristikum des *CRW* ist die Schwerpunkt-orientierte Formation, die aus der *RSSI* Prädiktion resultiert. Das Ergebnis ist ein Mangel an Explorationseffizienz. Vor diesem Hintergrund wurde der *Distributed Dispersion Detection Algorithm (DDD)* entwickelt. Der *DDD* analysiert die verfügbaren Informationen über Schadstoffgradienten in der Absicht eine agenten-basierte und dezentrale Trajektorienplanung vorzunehmen.

Die Suchstrategie erfolgt folgendermaßen:

1. Zufällige Suche nach Schadstoffen
2. Ansteuern der Zelle mit der niedrigsten Schadstoffkonzentration (c_{min})
3. Fortsetzen der Suche in der unbekanntenen Nachbarschaft von c_{min}

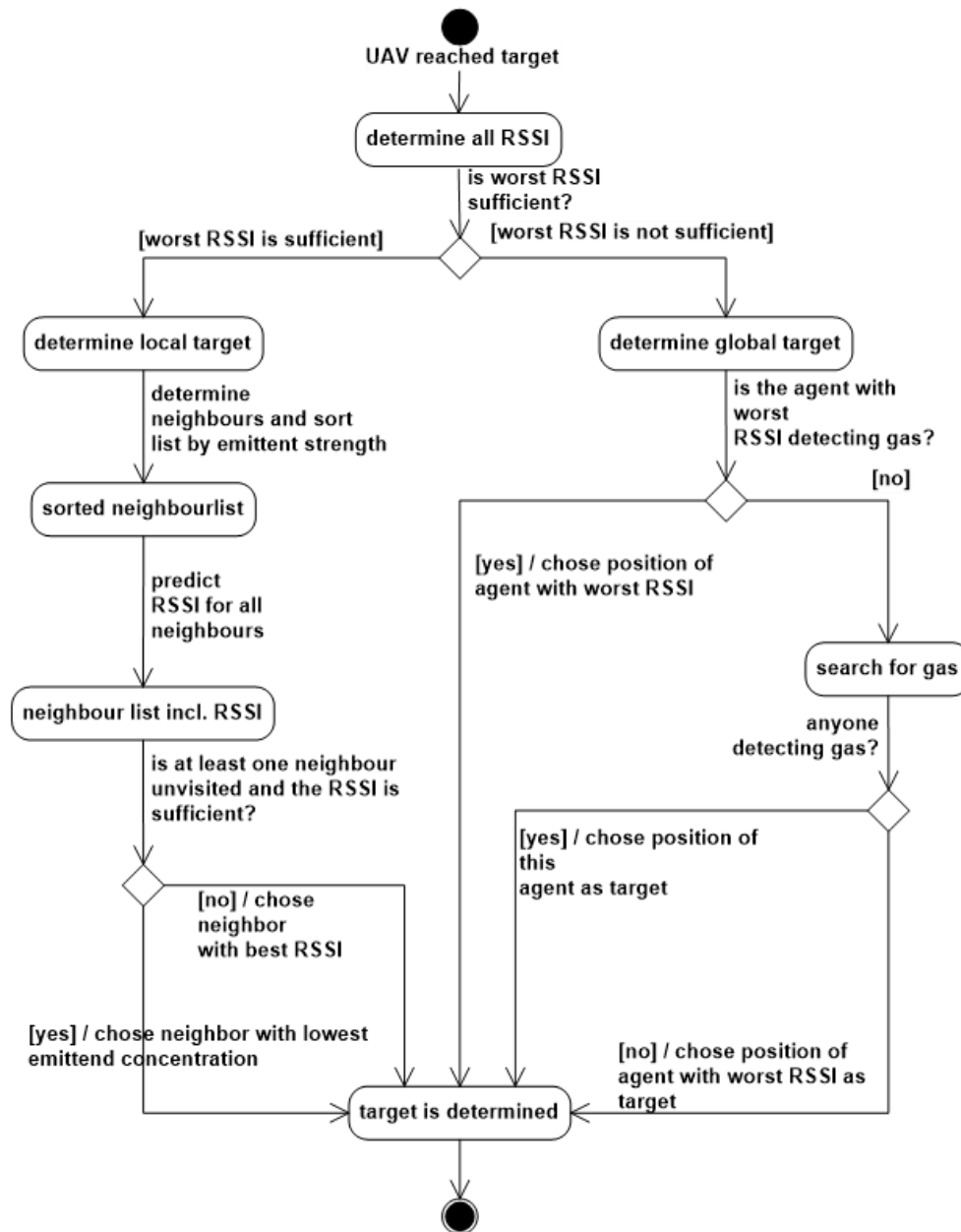


Abbildung 37: Zustandsdiagramm für den Distributed Dispersion Detection Algorithmus [2]

Zusätzlich zur individuellen Wahrnehmung eines Agenten, werden die gesammelten Informationen kontinuierlich innerhalb des Schwarms ausgetauscht. So können auch potentiell interessante Ziele in der Nähe von anderen Agenten erkannt werden.

Die Abbildung 37 zeigt das Zustandsdiagramm des *DDD*. Dieser Algorithmus integriert zwei verschiedene Ansätze abhängig von der aktuellen Qualität der Kommunikationsverbindung. Wenn ein Agent sein aktuelles Ziel erreicht hat, wird die Received Signal Strength (RSS) zu allen anderen UAVs geprüft. Angenommen der RSS ist ausreichend, dann soll der Agent seine lokale Suche fortsetzen. Der Modus Operandi ist der gleiche wie bei *ADCRW*.

Ist der RSS allerdings nicht ausreichend, dann ist es das Primärziel die Kommunikationsverbindung zu erhalten. Die lokale Suche wird abgebrochen und ein globales Ziel wird bestimmt. In der Absicht die Linkqualität zu erhöhen wird das UAV zu dem die schlechteste Verbindung besteht und das gleichzeitig Schadstoffe detektiert angefliegen. Auf diese Weise werden zwei Ziele erreicht: Kommunikation und Erkundung.

Analyse der Algorithmen

Erkundungsleistung der Grenzschicht

Im ersten Schritt wird die Erkundungsleistung der Schadstoff-Grenzschicht analysiert. In Abbildung 38 werden die Resultate für alle vier verwendeten Algorithmen dargestellt. mTSP und CRW dienen dabei als obere und untere Schranke. DDD und ADCRW erreichen final eine Erkundungsrate von über 95%. Allerdings gibt es einen auffälligen Unterschied im zeitlichen Verlauf der Erkundung. Nach 30 Minuten

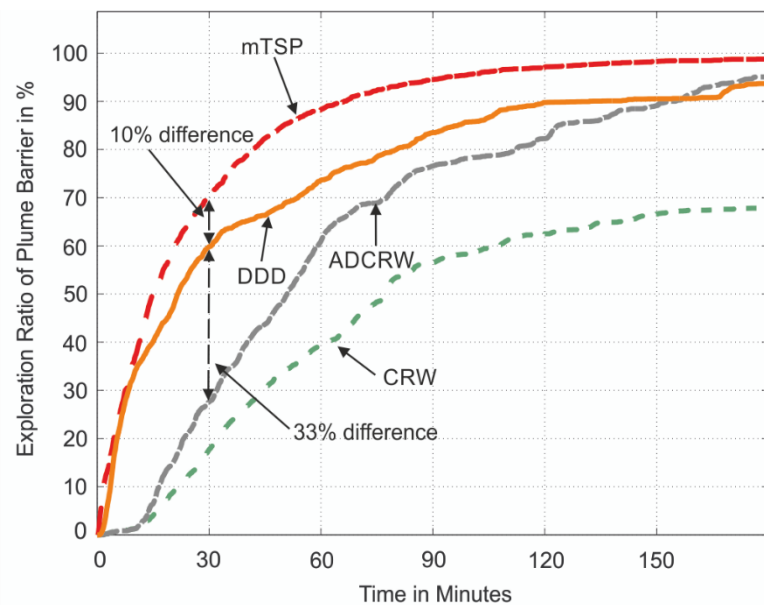


Abbildung 38: Erkundungsleistung der Grenzschicht. mTSP, DDD und ADCRW erreichen 95% bis nahezu 100% Erkundungsgrad. [2]

hat der ADCRW 27% der Grenzschicht erkundet, während der DD bereits 60% und der mTSP sogar 70% erkundet hat. Diese Lücke schließt sich mit fortlaufender Erkundung.

In Abbildung 39 ist der Fortschritt der Erkundung zu unterschiedlichen Zeitpunkten für den DDD dargestellt. Die grünen Punkte repräsentieren erkundete Grenzzellen, unbekannte Zellen sind rot dargestellt. Es wird deutlich, dass der DDD weite Teile der Grenzschicht innerhalb der ersten 30 Minuten erkundet. Nach ca. 120 Minuten ist das Grenzgebiet komplett erkundet.

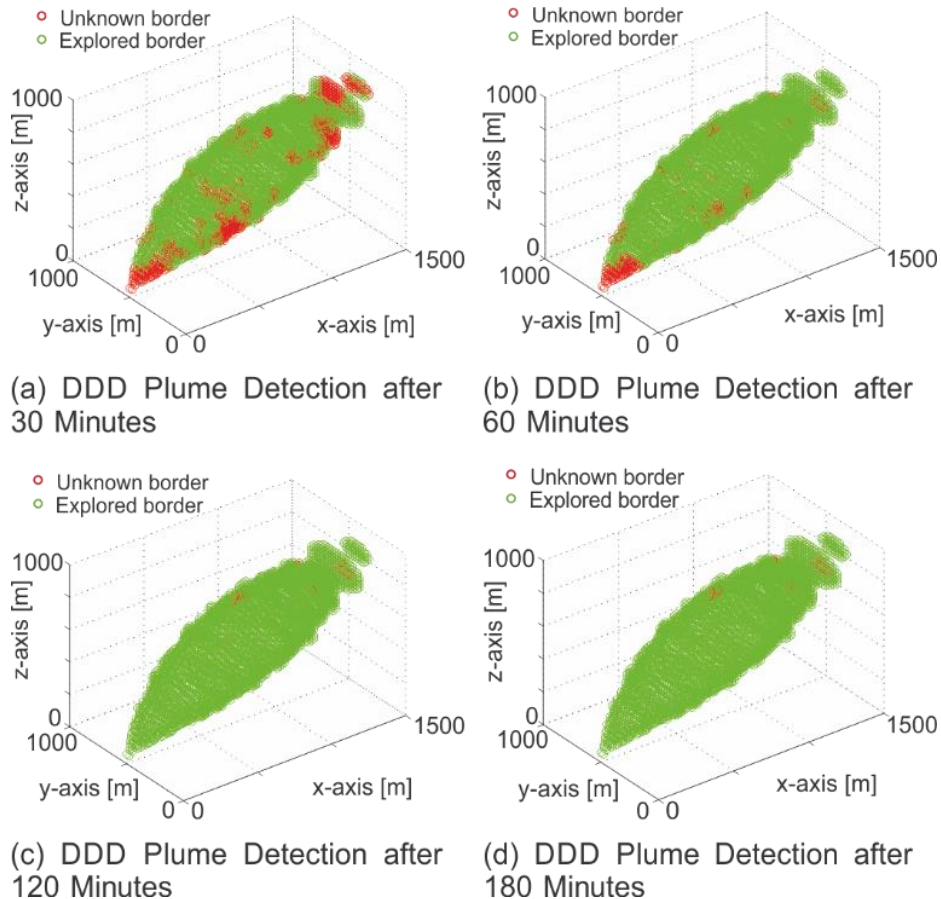


Abbildung 39: Fortschritt der Grenzschichterkundung mit dem DD – grüne Punkte stellen erkundete Bereiche dar, rote Punkte sind unbekannt. Der Großteil der Erkundung findet in den ersten 30 Minuten statt. [2]

Mesh Reliability Fulfillment

Wie zuvor erwähnt ist die Zuverlässigkeit der Mesh-Kommunikation eine Grundvoraussetzung für die Schwarmkooperation. Im Folgenden wird das Erscheinen von Clustern analysiert, also das Auseinanderfallen des Schwarms in mehrere Teile. Die Abbildung 40 zeigt die Zuverlässigkeit der Kommunikation im Schwarm. Der *DDD* erreicht nahezu 100% Verfügbarkeit, Clusterisierung tauscht nur sehr selten auf und wird sofort „geheilt“. Die Standardabweichung ist ebenfalls sehr gering. Ähnliche Resultate erreicht der *ADCRW*. Die Zuverlässigkeit liegt hier bei 96%. Der artverwandte *CRW* erreicht eine etwas höhere Kommunikationsleistung. Dies ist der höheren Komplexität des *ADCRW* geschuldet. Der *mTSP* hingegen, als einziger Algorithmus nicht communication-aware, erreicht eine Zuverlässigkeit von 21%. Es

treten also zahlreiche Separationen auf. Ein sicherer Schwarmbetrieb ist somit nicht möglich.

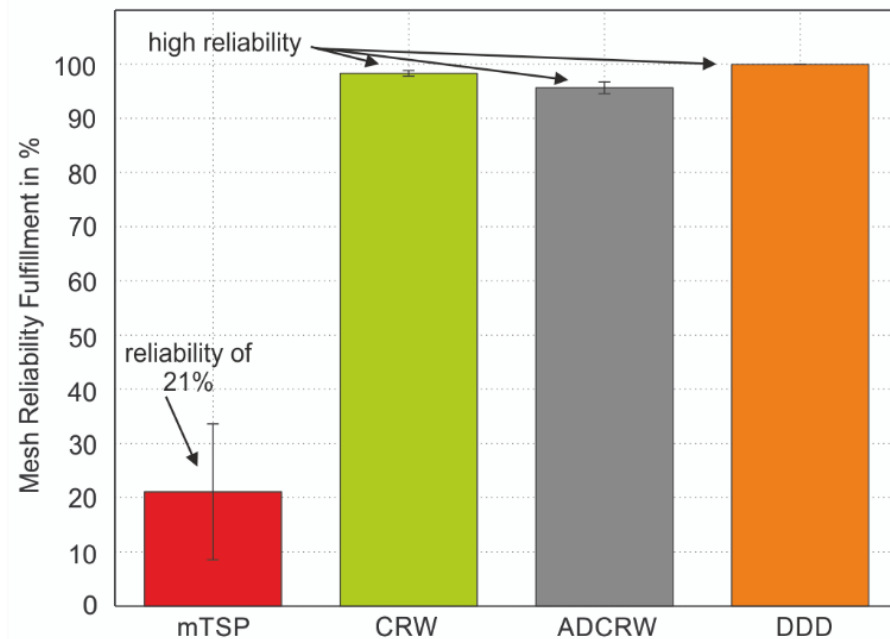


Abbildung 40: Mesh Reliability Fulfillment – Die drei communication-aware Algorithmen erhalten eine hohe Zuverlässigkeit im Gegensatz zu mTSP. [2]

In Abbildung 41 ist die Wahrscheinlichkeitsdichtefunktion für die durchschnittliche Anzahl von Verbindungen aller UAVs dargestellt. Wenn der DDD verwendet wird ist die Anzahl der Verbindungen bei 3,7. Da ein UAV maximal vier Verbindungen haben kann, ist der Schwarm also fast immer vollständig vermascht. Zu keinem Zeitpunkt existieren weniger als zwei Verbindungen. Der mTSP liefert im Durchschnitt 1,2 Verbindungen. Dies bedeutet, dass ein UAV meist nur mit einem einzigen anderen UAV verbunden

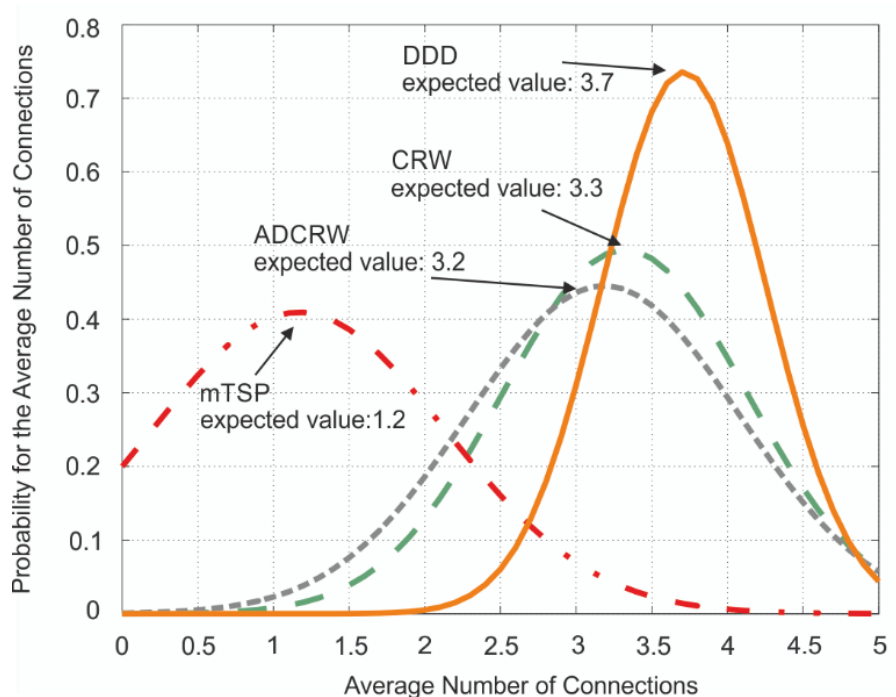


Abbildung 41: Wahrscheinlichkeitsdichtefunktion für die Anzahl der aktiven Verbindungen für alle UAVs. Der DDD zeigt nahezu vollständige Kohärenz, der mTSP hingegen erreicht nur eine geringe Anzahl von Verbindungen. [2]

ist. Das Maximum von vier Verbindungen wird nur zum Start erreicht. Nach einer kurzen Zeitspanne ist die Distanz zu groß für stabile Kommunikationsverbindungen. Der Schwarm ist also die meiste Zeit komplett separiert. Das bestätigt die vorherigen Ergebnisse. Die Resultate von *ADCRW* und *CRW* sind vergleichbar zu denen des *DDD*, wenn auch etwas schlechter. Alle drei kommunikations-sensitiven Algorithmen erzielen eine hohe Mesh Zuverlässigkeit.

Effizienz der Erkundung

Ein primäres Ziel der vorgeschlagenen Algorithmen ist es erneute Besuche bereits erkundeter Grenzzellen zu vermeiden, da dies ein bekannter Nebeneffekt von Random Walk-basierten Verfahren. Die Verteilung der Zellbesuche ist in Abbildung 42 für drei Algorithmen dargestellt. Dabei wird der Großteil der Zellen genau einmal besucht. Bei *DDD* trifft dies auf 70% der Zellen zu, bei *mTSP* und *ADCRW* auf ca. 80% der Zellen. Die verbleibenden Zellen werden teilweise bis zu 20-mal wiederbesucht. Die Resultate für den *CRW* können hier gefunden werden: [1]. Die Effizienz der neuen Algorithmen ist vergleichbar mit der von *mTSP*. Dies ist ein gutes Ergebnis, da der *mTSP* aufgrund seiner Vorplanung Wiederbesuche vermeiden möchte.

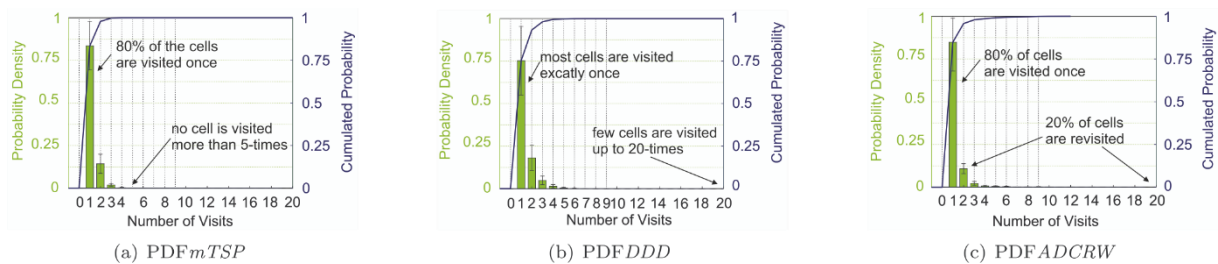


Abbildung 42: Anzahl der Besuche der Zellen nach 180 Minuten für die neuen Algorithmen. Alle drei Algorithmen weisen eine hohe Effizienz auf. [2]

Skalierbarkeitsanalyse

Während der Durchführung einer UAV Mission kann sich die Umgebung dramatisch verändern. Ein UAV kann beispielsweise eine Fehlfunktion erleiden oder muss aufgeladen werden. Die Skalierbarkeitsanalyse adressiert genau dieses Szenario. Nach 10 Minuten fallen zwei von fünf UAVs aus. Die Algorithmen müssen auf diese neue Situation reagieren und sich adaptieren. Wie in Abbildung 43 gezeigt ist der *mTSP* hiervon stark beeinflusst. Die vorkalkulierten Routen können nicht ohne Neustart des Algorithmus verändert werden. Daher erreicht der *DDD* nun das gleiche Level der Erkundungsleistung. Beide Algorithmen detektieren nahezu 90% der Grenzzellen innerhalb von 90 Minuten. Ein starker Einfluss kann ebenfalls bei der Erkundungsleistung des *ADCRW* erkannt werden. Mit diesem Algorithmus werden nach 90 Minuten nur mehr 60% der Zellen identifiziert. Im Gegensatz zu den anderen

Algorithmen reagiert der DDD also sehr robust auf den Ausfall zweier UAVs. Der mTSP verliert etwas an Effizienz, liefert aber nachwievor ein gutes Ergebnis.

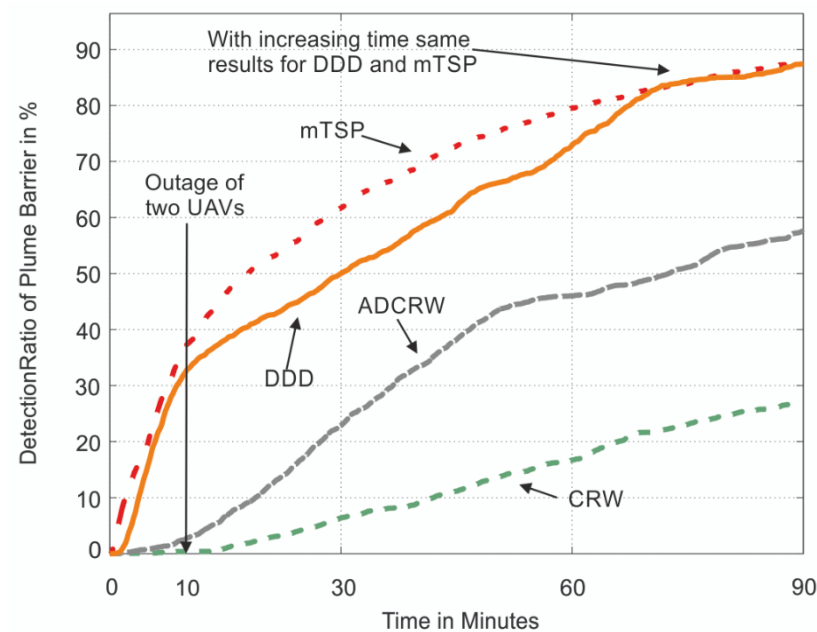


Abbildung 43: Erkundungsleistung der Grenzsicht bei einem Ausfall von zwei UAVs. Der DDD kann sich dieser Situation am besten anpassen. [2]

Schlussfolgerung

Zwei neue bzw. verbesserte Algorithmen, der DDD und ADCRW wurden in dieser Analyse vorgestellt. Die Strategien minimieren die Wechselwirkung zwischen Erkundungseffizienz und Kommunikationsbeschränkungen. Im Vergleich zu bereits bekannten Algorithmen wie mTSP und CRW erreichen die neuen Verfahren annähernd die gleiche Erkundungsleistung wie der mTSP während sie zugleich die Schwarmkohärenz wahren. Daher sind diese Algorithmen für die Grenzschichterkundung gut geeignet.

5.3 Multikriterielle Optimierung von Mobilitätsverhalten

Im vorherigen Kapitel wurden innovative Mobilitätsalgorithmen für autonome Roboter vorgestellt. Um die Lücke zwischen Simulation und realer Welt zu schließen werden vielfach anspruchsvolle Entwicklungsmethoden wie eine Kombination aus Modellbasierten Verfahren und Software- wie auch Hardware-in-the-loop Simulationen verwendet. Ein ungelöstes Problem bzgl. der Mobilität ist die Bestimmung der optimalen Parametrisierung für multiple Optimierungsziele. Vor diesem Hintergrund soll der Mobility Evaluation and Parameter Optimizer (MobEPO) eingeführt und analysiert werden. Multikriterielle Optimierungsalgorithmen werden verwendet um die optimalen Parametersets zu finden.

5.3.1 Mobility Evaluation and Parameter Optimizer

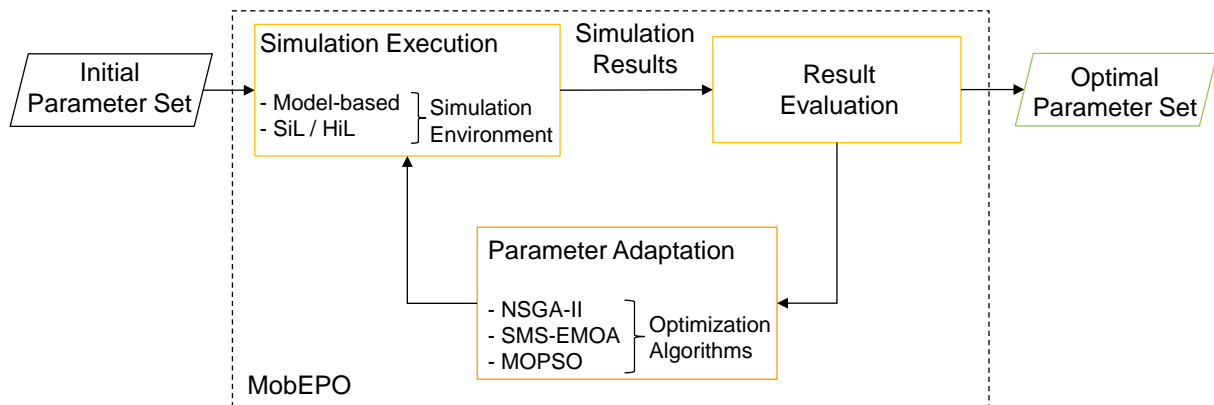


Abbildung 44: Funktionale Architektur von MobEPO [7]

In vorangegangenen Arbeiten wurde ein vier-phasiger Entwicklungsprozess vorgestellt, der eine modellbasierte multiskalare Simulation, Software- und Hardware-in-the-loop (SiL / HiL) Simulationen und eine Experimentalplattform vorsieht um kommunikations-sensitive Verhalten für kooperierende UAVs zu entwickeln.

Durch intensive Tests und Parameter Feedback konnte dadurch die Lücke zwischen simulieren und realen Flugergebnissen verkleinert werden. Doch ungeachtet dieses Fakts ist die zentrale Herausforderung des Bestimmens der optimalen Parameter für die kommunikations-sensitiven Algorithmen nachwievor ungelöst. Die MobEPO Methodik ist in der Lage metaheuristische Algorithmen für die Optimierung der Parametersets zu nutzen und dabei verschiedenartige Optimierungsziele zu beachten. MobEPO (vgl. Abbildung 44) arbeitet dabei wie folgt: Initial wird die Optimierer mit einem Parameterset gestartet, der aus Erfahrungswerten abgeleitet ist. Die Optimierer startet dann hierfür Simulationen. Sind diese Simulationen beendet werden die Ergebnisse in Bezug auf vorher festgelegte KPIs evaluiert. Im Parameter-Adaptionsschritt bestimmen die metaheuristischen Optimierungsalgorithmen eine neue Parameter-Population. Diese wird dann an das Simulation Execution Modul übertragen. Nach einem vorher festgelegtem Maximum von erzeugten Generationen oder wenn eine Sättigung in den Ergebnissen festgestellt werden, wird der Optimierungsprozess gestoppt.

Das Ziel der multikriteriellen Optimierung ist es ein Parameterset zu finden, dass den besten Kompromiss zwischen allen KPIs aufweist. Der generelle Ansatz ist es eine Zielfunktion für jeden KPI a priori zu definieren und diese dann nach einer zugehörigen Gewichtungsfunktion zu maximieren oder zu minimieren. Die Herausforderung liegt im Vergleich des Lösungsraums der verschiedenen Optimierungsmethoden um den Besten auszuwählen. Daher muss der Lösungsraum in Metriken überführt werden, welche die Qualität der Lösung bestimmen, z.B. die Distanz der Pareto-Front. Ein häufig genutzter und allgemein als fair angesehener Ansatz ist die sogenannte S-

Metrik, welche ein Maß für das dominante Hypervolumen ist. Wenn die S-Metrik maximiert wird zeigt sich der Lösungsraum.

In dieser Evaluierung werden bekannte Algorithmen wie S-Metric-Selection-EMOA (SMS-EMOA), NSGA-II und Multi-Objective Particle Swarm Optimization (MOPSO) verwendet.

Wie zuvor angedeutet, erfordert die Definition der Zielfunktionen Fachwissen und Einblick in die Ziele der Optimierung. Zusätzlich ist festzuhalten, dass die meisten verfügbaren Optimierungsalgorithmen für Optimierungsfunktionen höherer Ordnung (z.B. mit mehr als drei konkurrierenden Optimierungszielen) nicht gegen die Pareto-Front konvergieren. Die meisten modernen EMOA Algorithmen wie der SMS-EMOA nutzen primär ein Pareto-dominiertes Auswahlkriterium und sekundär ein Kriterium welches nur auf Individuen angewendet wird, welche nach der primären Auswahl gleich sind.

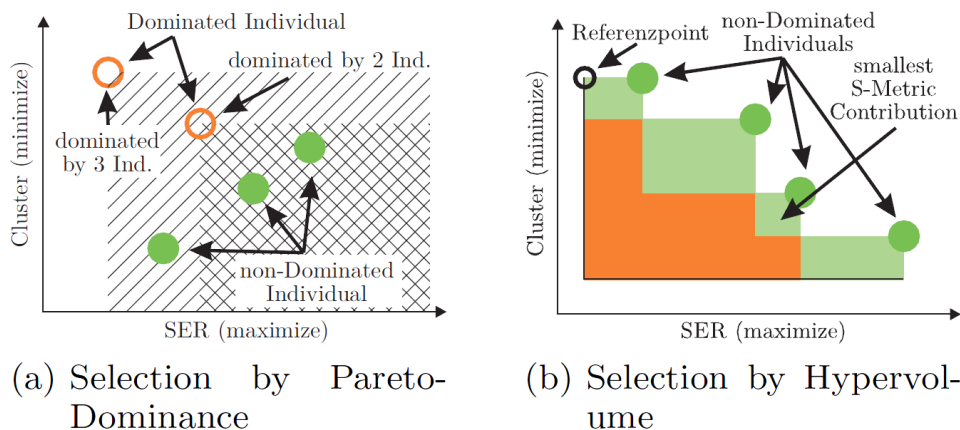


Abbildung 45: Pareto-Dominanz und Hypervolumen-Auswahl für zwei Optimierungsziele [7]

Das primäre Kriterium teilt die Population in dominierte und nicht-dominierte Individuen. Falls die Population dominierte Lösungen enthält, werden die meist dominierten (und somit schlechtesten) Lösungen entfernt, siehe hierzu Abbildung 45a. Falls keine dominierten Lösungen existieren, wird die Lösung mit der kleinsten S-Metrik entfernt, vgl. Abbildung 45b.

Wenn alle Individuen einer Population evaluiert wurden ist der nächste Schritt eine neue Population zu erstellen. In dieser Phase kommen evolutionäre Methoden wie Rekombination und Mutation zum Einsatz. Die genaue Methode hängt vom verwendeten Algorithmus ab.

5.3.2 Vergleich der Optimierungsalgorithmen

In der durchgeführten Evaluation sind die evolutionären Algorithmen angehalten nach 60 Permutationsschritten eine Lösung zu finden. Der erste Vergleich die Verteilung der Lösungen während der Entwicklung der Optimierung. Bezugnehmend auf die Optimierungsziele wie sie zuvor definiert wurden, ist eine gute Lösung wenn der

Schwarm kohärent und die Erkundungsleistung (SER) so hoch wie möglich ist. Die Abbildung 46 zeigt die Entwicklung des SER für jeden Optimierungsschritt. Dabei erfüllt jede in Form einer Linie gezeigte Lösung das Ziel der Schwarmkohärenz während einzelne Punkte die Ergebnisse von Läufen darstellen, in denen das Ziel der Schwarmkohärenz nicht erreicht wurde.

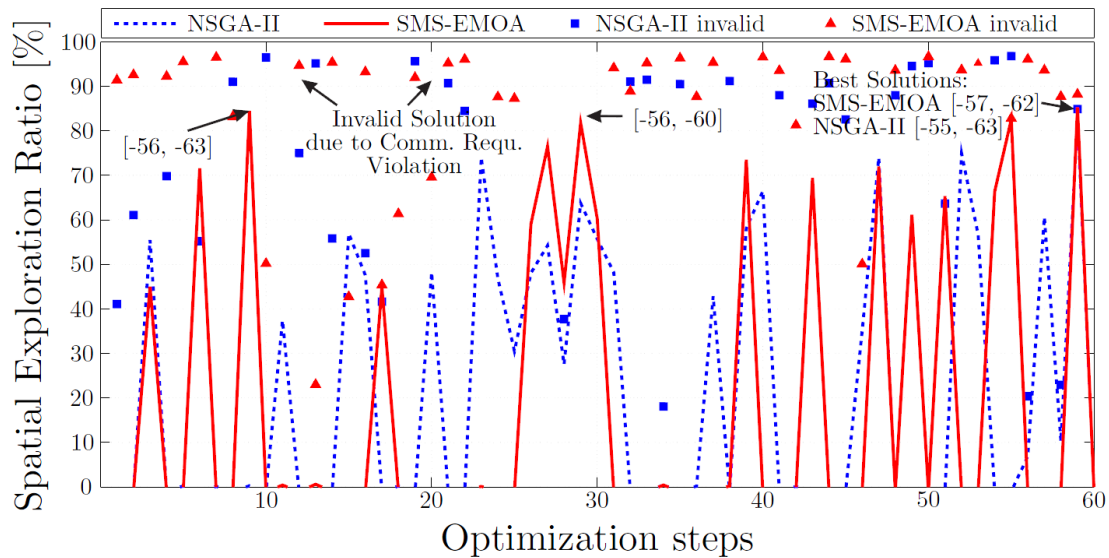


Abbildung 46: Entwicklung der Erkundungsleistung (SER) während der Optimierung [7]

Beide Algorithmen, SMS-EMOA wie auch NSGA-II, finden Lösungen welche die Anforderungen erfüllen. Es ist interessant zu sehen, dass die Algorithmen nicht kontinuierlich valide Lösungen gefunden haben. Stattdessen gibt es auch Ergebnisse mit hohem SER aber Verletzung der Kommunikationsanforderungen. Diese Lösungen sind von weiteren Permutationen ausgeschlossen. Aus der Abbildung kann geschlussfolgert werden, dass der SMS-EMOA nahezu optimale Lösungen zu Beginn, in der Mitte und am Ende findet. Wenn die gleiche Anzahl an Iterationen verwendet wird, erreicht NSGA-II ebenfalls gute Lösungen. Am Ende sind die gefundenen Parametersets und Erkundungsergebnisse nahezu identisch. SMS-EMOA findet die beste Lösung mit 84.1% SER bei den Parametern $RSS_{min} = -62 \text{ dBm}$ und $RSS_{max} = -57 \text{ dBm}$. NSGA-II findet die beste Lösung mit 84.9% SER bei den Parametern $RSS_{min} = -63 \text{ dBm}$ und $RSS_{max} = -55 \text{ dBm}$.

In Abbildung 47 werden die besten Ergebnisse für alle drei Optimierungsverfahren hinsichtlich der Erkundungsleistung dargestellt. Das beste von MOPSO gefundene Parameterset ist -49 dBm für RSS_{max} und -59 dBm für RSS_{min} . Damit wird ein SER von 73% erreicht. Um die Korrektheit dieser Lösung zu bestätigen und zufälliges Verhalten auszuschließen wird jede Simulation fünfmal durchgeführt. Das Konfidenzintervall für 95% wird ebenfalls dargestellt. Für NSGA-II und SMS-EMOA variieren die Ergebnisse nach 90min um ungefähr 3%. Die Variation für MOPSO ist größer, was den Eindruck bestätigt, dass MOPSO innerhalb von 60 Iterationen das Optimum nicht finden konnte.

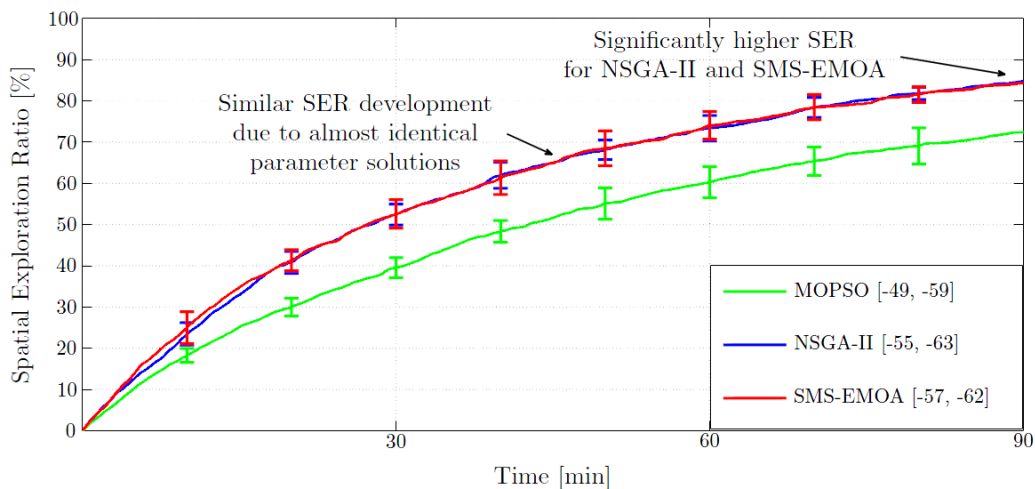


Abbildung 47: Erkundungsleistung dreier Verfahren nach Optimierung [7]

Die Schwankung des SER für alle gefundenen Lösungen der Optimierungsverfahren wird in Abbildung 48 gezeigt. SMS-EMOA hat viele Parametersets gefunden, die einen hohen SER erzielen. Das Verteilungsmuster für MSGA-II und MOPSO ist viel größer.

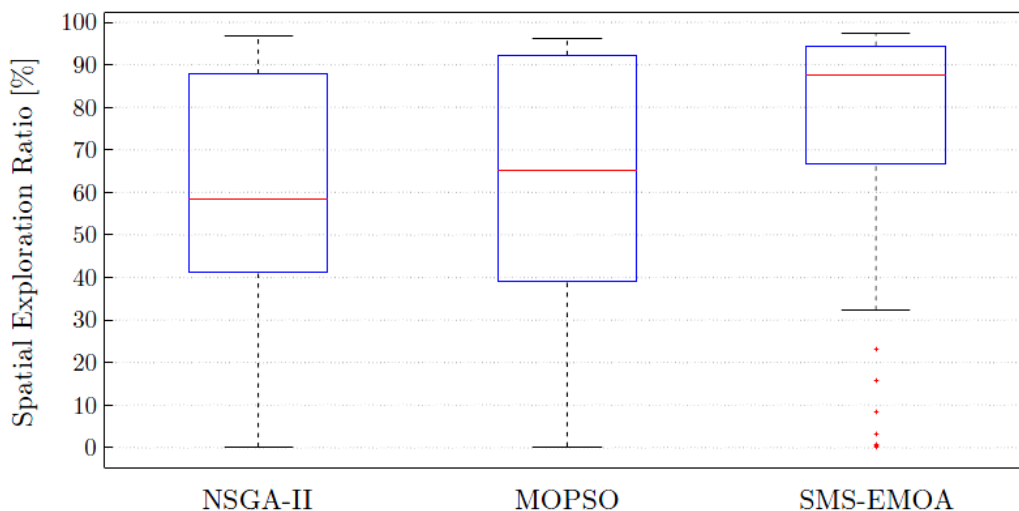


Abbildung 48: Schwankung des SER für die drei betrachteten Optimierungsverfahren [7]

Das dritte Ziel ist eine niedrige Anzahl von Topologieveränderungen zu erreichen um den Overhead, der durch das Verwalten des Netzes entsteht, wie z.B. Route Updates, zu minimieren. Eine Topologieveränderung bedeutet, dass eine existierende Kommunikationsverbindung zwischen zwei UAVs abbricht oder eine neue hinzukommt. In Abbildung 49 ist die CDF für die Lebensdauer der Topologien dargestellt. Die stabilste Topologie wird durch die Lösung von MOPSO erreicht. Die Topologie bleibt für mehr als eine Stunde unverändert. Bei NSGA-II und SMS-EMOA existieren die meisten Topologien für ungefähr 100 s. Das bewirkt andersrum einen höheren SER aufgrund schwächeren RSS Grenzen. Dadurch wird die Distanz zwischen UAVs größer was eine Erhöhung des SER bewirkt aber gleichzeitig die Gefahr von Verbindungsabbrüchen erhöht.

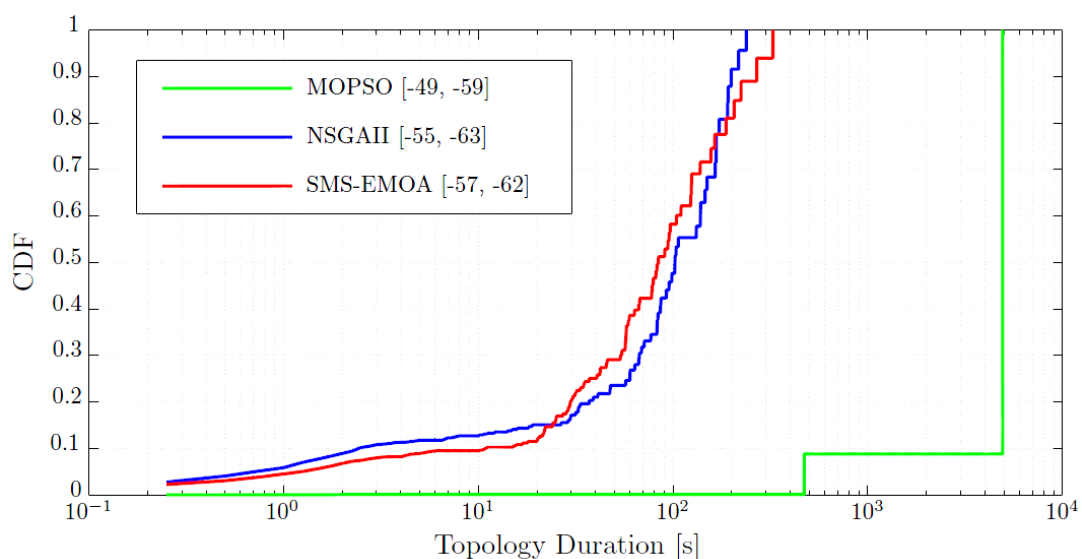


Abbildung 49: CDF der Topologielebensdauer für die jeweils besten Lösungen [7]

Die Ergebnisse zeigen, dass die beste gefundene Lösung nicht für alle möglichen Szenarien die beste Lösung sein muss. Die hier vorgestellten Ergebnisse betrachten ein herausforderndes urbanes Szenario mit Hindernissen. Die Hindernisse haben einen starken Einfluss auf die Exploration ebenso wie auf die Schwarmkohärenz. In diesem Szenario werden zwei verschiedene Arten von Hindernissen benutzt. Hindernisse direkt oberhalb des Bodens repräsentieren Häuser, diese können nicht durchfliegen werden und dämpfen alle Kommunikation um 30 dB. Die Hindernisse in der Luft repräsentieren dagegen „Funklöcher“, sie sind befliegbar und dämpfen die Kommunikation um 10 dB.

In der Absicht den Einfluss verschiedener Kommunikationsumgebungen zu bestimmen, werden zusätzliche Simulationen mit typischen Parametern für ein städtisches und ein ländliches Szenario durchgeführt. Hierbei kommen keine Hindernisse zur Anwendung. In der Tabelle 4 werden die Ergebnisse dieser Studie präsentiert: Während der SER sehr vergleichbar ist (96% zu 97%), weichen die gefundenen Parameter stark voneinander ab. In der ländlichen Umgebung ist der

RSS_{min} bei -82 dBm , was nahe an der Abbruchgrenze für eine Verbindung von -83 dBm ist. Da es in diesem Szenario keine weiteren Störeinflüsse gibt ist dies verständlich. Im städtischen Szenario müssen die Parameter hingegen angepasst werden. Der RSS_{max} ist -63 dBm und der RSS_{min} ist -65 dBm .

Tabelle 4: Optimierungsergebnisse in verschiedenen Kommunikationsumgebungen [7]

Scenario 1 – Rural	
Parameter	Value
Channel Model	Friis transmission equation
Attenuation coefficient	2.3
Small scale fading model	none
Steeringparameter	$[-82, -85]$
Scenario 2 – Urban	
Parameter	Value
Channel Model	Friis transmission equation
Attenuation coefficient	3.5
Small scale fading model	Lognormal with 5 dB
Steeringparameter	$[-63, -65]$

5.4 Dynamisches Rollen-Management

Ein Ziel des ANCHORS Systemdesigns ist eine kontinuierliche Missionsdurchführung zu ermöglichen. Daher kommt der Überwachung des Status der Schwarmentitäten sowie deren Verhaltenssteuerung eine besondere Bedeutung zu.

Zwei Aspekte sind im Fokus des Swarm Health Management

- Überwache den Gesundheitsstatus aller Entitäten und reagiere ggfls. darauf. Daher muss ein Austauschprozess für Roboter vorgesehen sein.
- Implementierung eines kooperativen Start- und Landeprozesses um korrektes und sicheres Verhalten zu gewährleisten.

5.4.1 Autonome Start- und Landeprozesse mit Dynamic Role Management

Ein komplexes Rollenmanagement ist verantwortlich für die korrekte Ausführung von Starten und Landen. Die Herausforderung ist, das Rollenverhalten auf verschiedenen autonom agierenden Entitäten zu koordinieren. In ANCHORS kommt keine zentrale Entscheidungseinheit zum Einsatz, alles wird dezentral entschieden. Daher müssen

im Schwarm alle notwendigen Informationen ausgetauscht werden um die Agenten in die Lage zu versetzen selbständig Entscheidungen treffen zu können.

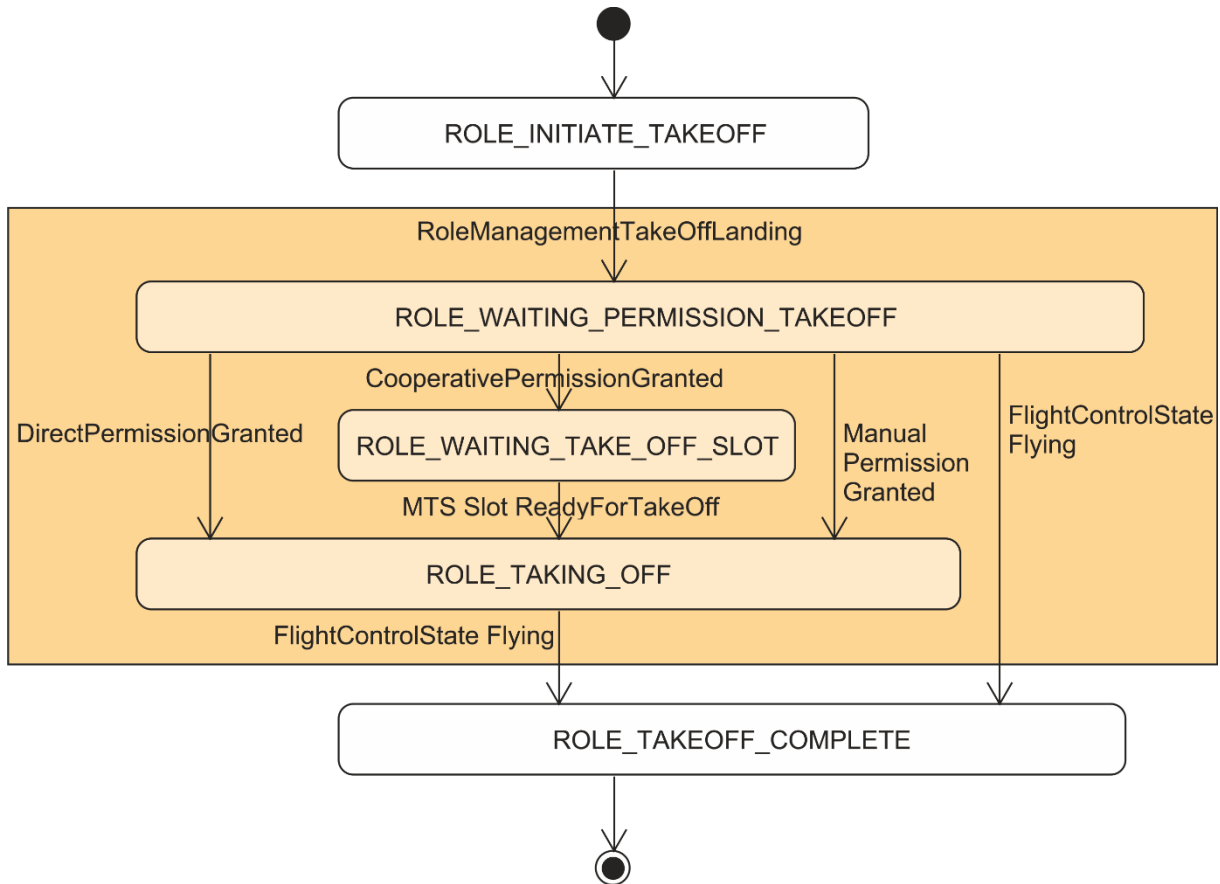


Abbildung 50: Role Management für den Startvorgang (Quelle: TU Dortmund)

In der Abbildung 50 wird der Workflow der Startprozedur gezeigt. Ausgangspunkt ist die Definition einer abstrakten Missionaufgabe durch den Benutzer. Dies könnte beispielsweise eine nukleare Erkundungsmision sein oder auch die Videoobservierung einer bestimmten Situation. Das Schwarmsystem koordiniert selbständig die Ausführung des Tasks, dabei prüfen die UAVs ihre Eignung für den Task und übernehmen diesen. Wenn ein UAV die Aufgabe übernommen hat wechselt seine Rolle in `ROLE_INITIATE_TAKEOFF`, dieser Rollenwechsel wird von dem MTS detektiert, welches nun die Startplattform vorbereitet. Als erstes rotiert die Plattform in die korrekte Position (ein UAV soll immer aus einer bestimmten Position heraus starten), dann muss das MTS die Halteklammern des UAV lösen. Zur gleichen Zeit überwacht das UAV die anderen Aktivitäten im Schwarm. Wenn ein anderes UAV im Landeanflug ist, geht das wartende UAV in die Rolle `ROLE_WAITING_PERMISSION_TAKEOFF` über, sonst wechselt es in die Rolle `ROLE_WAITING_TAKE_OFF_SLOT`. Wenn das MTS fertig ist und kein UAV stören

könnte, startet das UAV. Wenn eine Flughöhe von 15m erreicht ist gilt der Startvorgang als abgeschlossen.

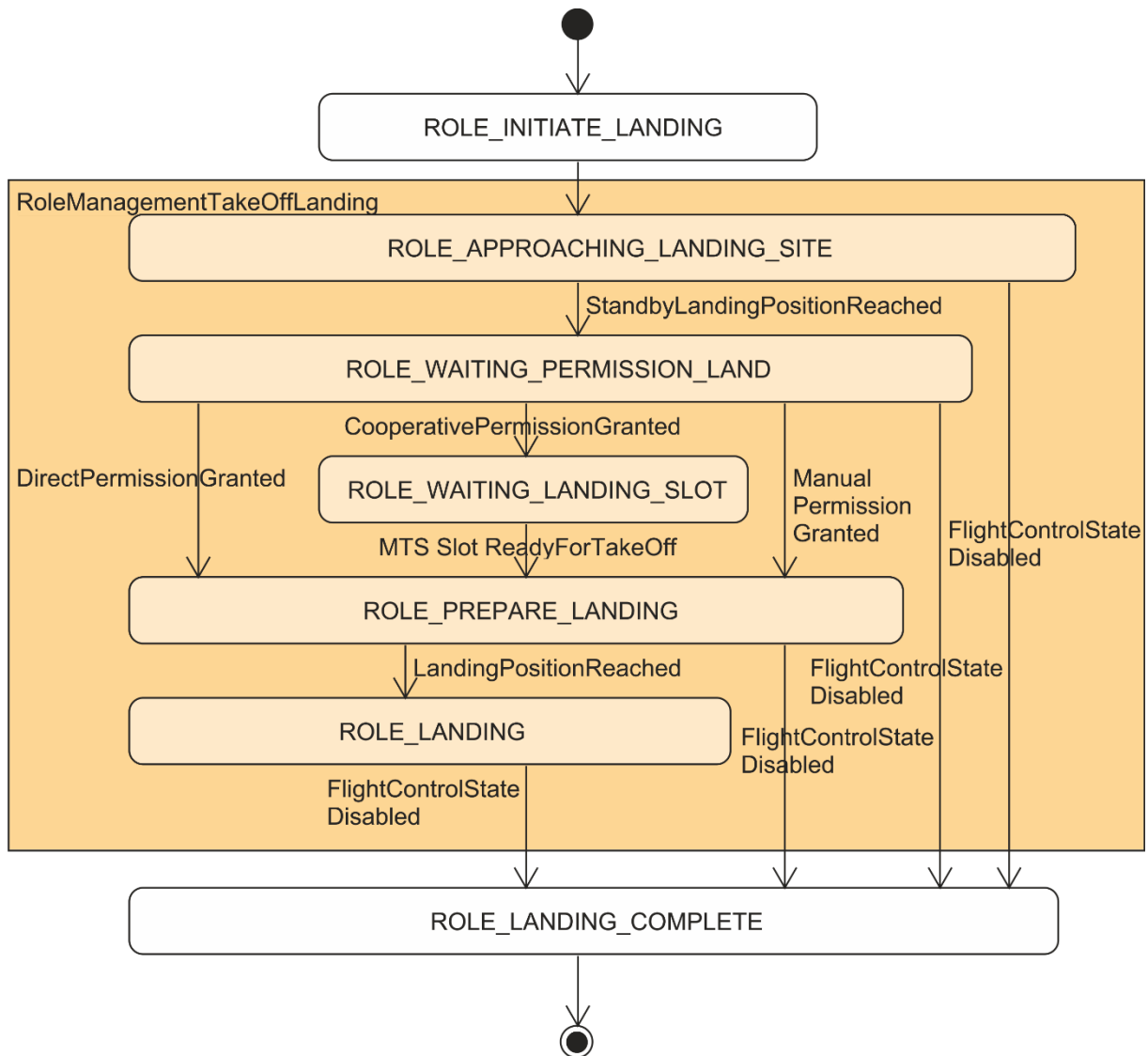


Abbildung 51: Role Management für den Landevorgang (Quelle: TU Dortmund)

Ein vergleichbarer Ansatz wird für den Landevorgang gewählt. Der Landeprozess wird initiiert wenn der Ladestand der Batterie eines UAV ein vordefiniertes Niveau unterschreitet. Das UAV fliegt zum MTS um aufzuladen (*ROLE_APPROACHING_LANDING_SITE*). Das MTS bemerkt den Landewunsch automatisch und startet die Vorbereitungen für einen freien Landeplatz. Wenn das UAV das MTS erreicht bleibt es in einer Warteposition außerhalb des Start- und Landebereichs bis es die Erlaubnis des MTS erhält zu landen (*ROLE_WAITING_PERMISSION_LAND*). Wenn der Landeplatz vorbereitet ist, nähert sich das UAV dem MTS (*ROLE_PREPARE_LANDING*). Das schwarm-basierte Fliegen wird ausgeschaltet und das AUTOLAND übernimmt die Steuerung (*ROLE_LANDING*). Ein vollzogener Landevorgang wird vom MTS und vom UAV

registriert und gemeldet. Erst wenn beide Meldungen eingegangen sind, können andere Aktionen ausgeführt werden.

5.4.2 Kontinuierliche Missionsdurchführung

Wie bereits beschrieben wird der Status jedes Roboters kontinuierlich überwacht, dazu gehört auch der Ladestand der Batterie. Zum Aufladen fliegt das UAV zum MTS und landet dort wie zuvor dargestellt automatisch. Um eine reibungslose Fortsetzung der Mission zu gewährleisten ist es aber erforderlich dieses UAV zu ersetzen.

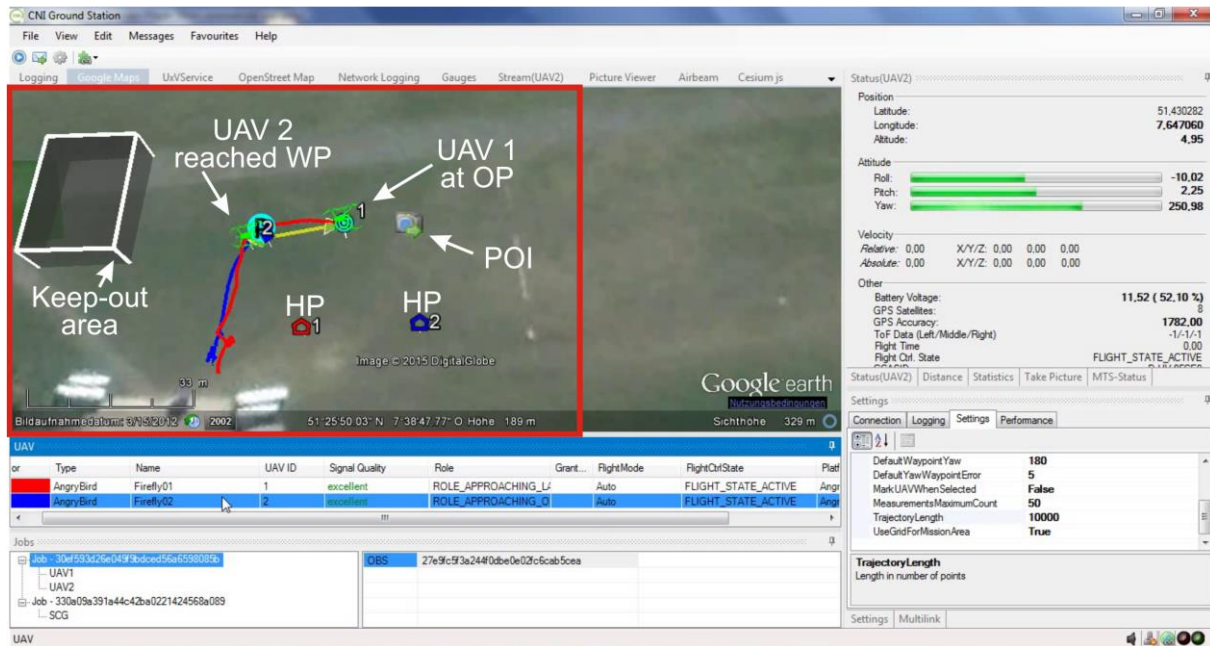


Abbildung 52: Unterbrechungsfreie Ausführung eines Beobachtungstasks

(Quelle: TU Dortmund)

In Abbildung 52 wird eine beispielhafte Mission dargestellt. Die UAVs haben die Aufgabe eines point-of-interest (POI) zu observieren. Dafür wird ein Observing Point (OP) sowie eine Warteposition (WP) definiert. An diesen Koordinaten wartet ein zweites UAV um die Aufgabe zu übernehmen falls das erste UAV zurückfliegen muss.

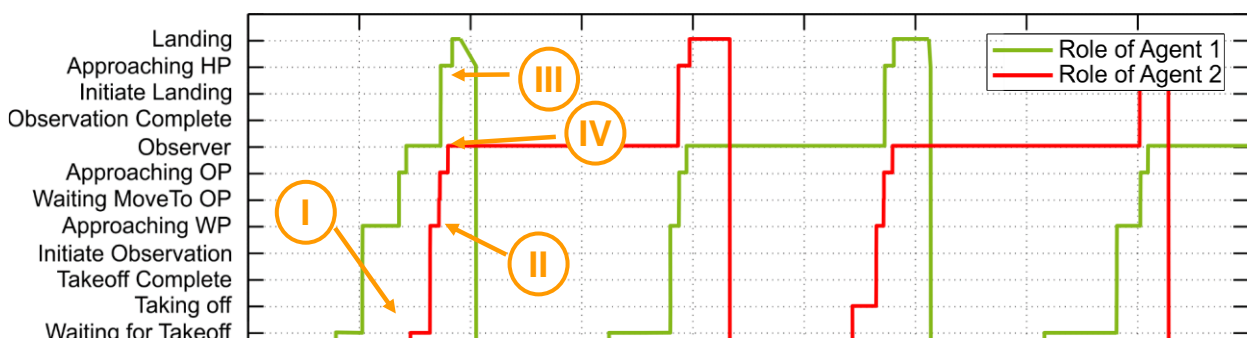


Abbildung 53: Eingenommene Rollen während einer unterbrechungsfreien Mission

(Quelle: TU Dortmund)

Die verschiedenen Rollen, welche von den UAVs während der Mission eingenommen werden, sind in Abbildung 53 zu sehen. Nach dem Start erreicht Agent 1 die Warteposition und fliegt dann weiter zum Observing Point. Zum Zeitpunkt I startet Agent 2 und fliegt zum Wartepunkt. Zum Zeitpunkt II übernimmt Agent 2 die Rolle „Waiting MoveTo OP“ weil der OP durch Agent 1 blockiert ist. Wenn der Ladestand der Batterie von Agent 1 unter ein bestimmtes Niveau fällt (Zeitschritt III) beendet der Agent seine Beobachtung und fliegt zum MTS zurück. Zur gleichen nähert sich Agent 2 dem OP und übernimmt, sobald er dort eingetroffen ist, die Beobachtungsmision (Zeitschritt IV). Die Abbildung 54 zeigt eines von zahlreichen Flugexperimenten um die kontinuierliche Missionsausführung zu testen.

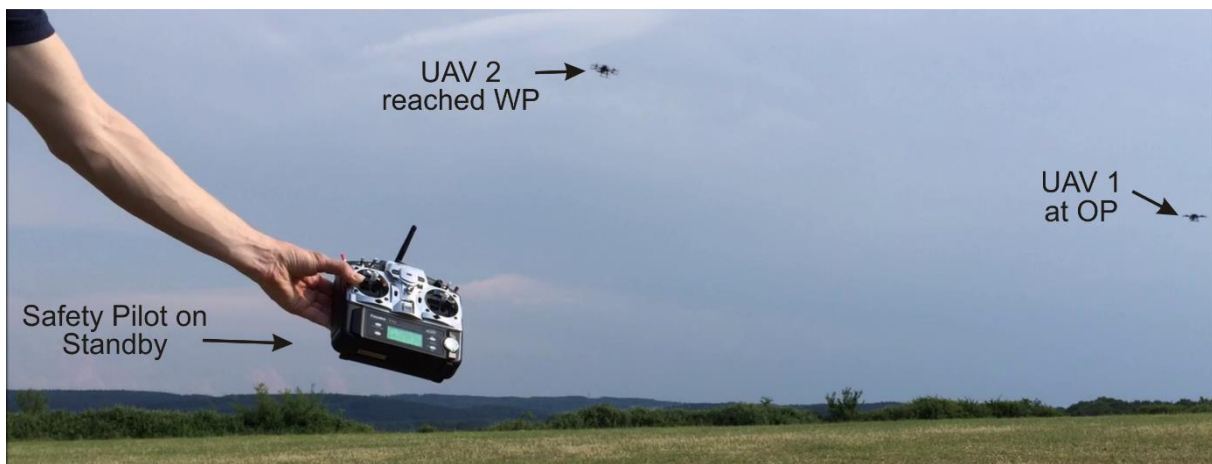


Abbildung 54: Flugexperimente zum Testen der kontinuierlichen Missionsausführung
(Quelle: TU Dortmund)

6. AP 6 – Platform Integration & System Validation

In diesem Arbeitspaket werden die entwickelten Komponenten der einzelnen Arbeitspakete in ein Gesamtsystem integriert und insbesondere in der Großübung der Feuerwehr validiert.

Zuvor wurden bereits im Rahmen des Early Demonstrators Teilaspekte des Systems vorgestellt.

6.1 Meilenstein 1 – Early Demonstrator

Zur Hälfte der Laufzeit des Projekts nach 18 Monaten wurde in Saclay bei Paris das erste Meilensteintreffen abgehalten. Dabei wurden von den einzelnen Partners Komponenten in Form eines Early Demonstrator vorgestellt.

Für die TU Dortmund standen dabei folgende Aspekte im Vordergrund:

- In einer Hardware-in-the-loop (HiL) Simulation wurde der kooperative Einsatz mehrerer Schwarmagenten wie UAVs und UGVs gezeigt. Die Visualisierung

der simulierten Bewegung und die Steuerung des Schwarmsystems erfolgte dabei bereits mittels der Steuerungskomponente des Schwarmsubsystems.

- Die Integration des UGV Austauschsystems wurde demonstriert und bereits in das kooperative Schwarmverhalten übernommen.
- In einer Simulation wurden die Mobilitätsalgorithmen zur Sicherstellung der Kommunikation innerhalb des Schwarms und zur Sensorerfassung eines unbekanntes Gebiets demonstriert.
- Die Demonstration des kooperativen Schwarmverhaltens beinhaltete auch ein Experiment, dass die Verwendung von Professional Mobile Radio (PMR) über das ad-hoc WLAN Mesh des ANCHORS Systems zeigte.



**Abbildung 55: Videoübertragung in Real-Zeit über das WLAN Mesh beim Early Demonstrator
(Quelle: TU Dortmund)**

6.2 Meilenstein 2 – Großübung in Dortmund

Im Rahmen einer Großübung der Feuerwehr wurden die Ergebnisse des Projekts nach 36 Monaten vorgestellt und demonstriert.

Die Großübung fand auf dem Gelände der ehemaligen Westfalenhütte in Dortmund statt. Ausgangspunkt des Szenarios war ein Verkehrsunfall mit einem Transporter, der gefährliche Chemikalien geladen hat. In Folge der freigewordenen Substanzen mussten nahe gelegene Arbeiten mit einer Materialprüfungsquelle abgebrochen und

die Quelle unbeaufsichtigt zurückgelassen werden. Die Aufgabe des ANCHORS Systems war es mithilfe der UAVs eine Karte der radioaktiven Strahlung zu erstellen und damit die Quelle zu finden, zu identifizieren und ihre Gefährlichkeit einzuschätzen. Es kamen zwei mit Sensoren ausgestattete UAVs zum Einsatz, ein weiteres UAV sowie diverse Bodenroboter waren mit Kameras ausgestattet. Während der Übung war das Content-aware Hybrid Communication System bestehend aus dem WLAN Mesh und einer eigenständigen LTE Zelle in Betrieb.

Die Resultate der Übung wurden von den Endanwendern positiv aufgenommen, bereits während der laufenden Übung bat der Einsatzleiter der Feuerwehr um weitere Luftaufnahmen auch von dem eigentlichen Verkehrsunfall, da sich die ersten Aufnahmen als sehr hilfreich erwiesen haben.



Abbildung 56: Einsatz des ANCHORS Systems während der Großübung (Quelle: TU Dortmund)

6.3 Meilenstein 3 – Abschluss der Verlängerungsphase

Das Projekt wurde über die geplante Projektlaufzeit von 36 Monaten hinaus um sechs weitere Monate verlängert. Der Schwerpunkt der Arbeiten in dieser Zeit lag auf der Durchführung von Tests zur Systemvalidierung sowie der Sicherstellung der Projektergebnisse nach Beendigung der Förderung.

Um das ANCHORS System auch im Nachgang präsentieren zu können hat der Projektpartner KHG eine Grundversion des Systems bei sich aufgebaut. Da einzelne Komponenten nicht vollumfänglich dauerhaft zur Verfügung stehen wurde das System reduziert. Zu den nicht verfügbaren Komponenten gehören beispielsweise die eigenständige LTE Zelle, da die Funklizenz den Betrieb auf den Campus der TU Dortmund einschränkt.

Die Abbildung 57 zeigt die Komponenten des ANCHORS Systems. Die Kommunikation erfolgt über das WLAN Mesh. Auf Hinweis der Endanwender wurde

die Steuerung und Kontrolle des Schwarms auf einem Tablet-PC ermöglicht. So kann das System auch mobil, unter Reduzierung des logistischen Aufwands betrieben werden.

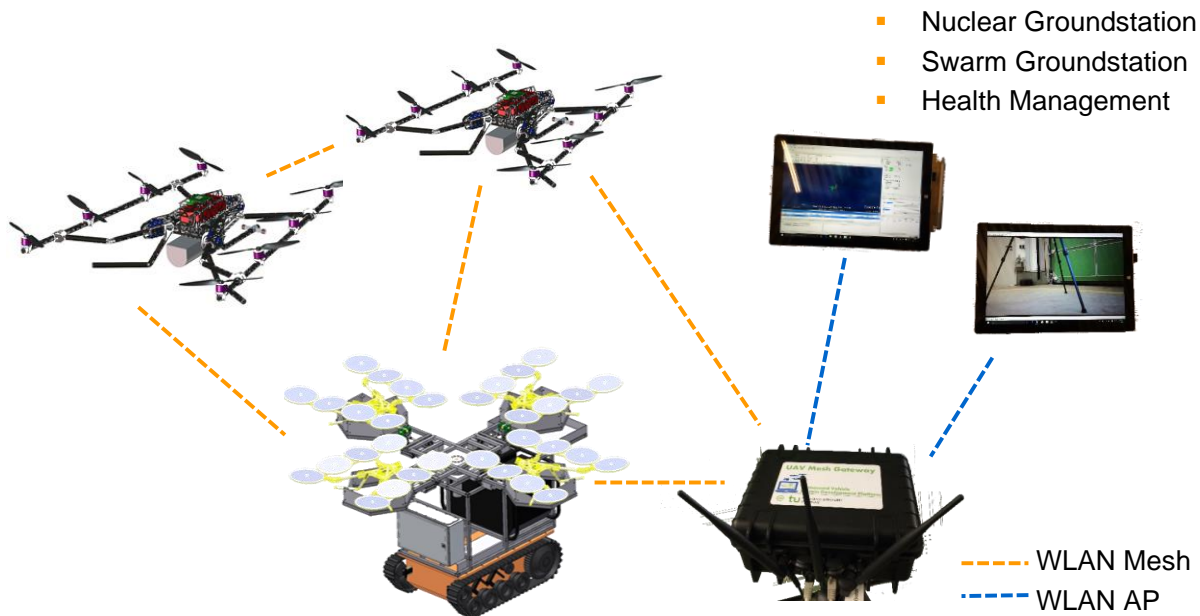


Abbildung 57: ANCHORS Systemdemonstrator nach Abschluss des Projekts
(Quelle: TU Dortmund)

6.4 Übersicht der Integrationsmeetings

Während der Projektlaufzeit gab es eine Vielzahl von Integrationsmeetings mit Beteiligung mindestens zweier Partner. Die folgende Tabelle gibt eine Übersicht der Meetings mit Beteiligung der TU Dortmund.

Tabelle 5: Übersicht der Integrationsmeetings

Meeting	Datum	Ort
Integration- und Validierung	23.10.2013 - 24.10.2013	Eggenstein-Leopoldshafen
Meilenstein 1	25.11.2013 – 28.11.2013	Paris
Integration- und Validierung	27.01.2014	Dortmund
Integration- und Validierung	18.06.2014 - 19.06.2014	Münster
Integration- und Validierung	13.10.2014 - 16.10.2014	Eggenstein-Leopoldshafen
WP 6 – Planung der Übung	20.11.2014	Dortmund
Integration- und Validierung	02.02.2015 - 05.02.2015	Eggenstein-Leopoldshafen
Integration- und Validierung	23.03.2015 - 27.03.2015	Eggenstein-Leopoldshafen
Integration- und Validierung	14.04.2015 - 17.04.2015	Dortmund

Meilenstein 2	18.04.2015	Dortmund
Integration- und Validierung	20.10.2015 – 21.10.2015	Eggenstein-Leopoldshafen
Meilenstein 3	22.10.2015	Eggenstein-Leopoldshafen

7. Zahlenmäßiger Nachweis der wichtigsten Positionen

In diesem Abschnitt werden die wesentlichen aus ANCHORS Mitteln getätigten Investitionen zusammen mit der Erläuterungen zur Verwendung im Projekt vorgestellt.

Flugroboter von Ascending Technologies

Während der Laufzeit des Projekts wurden vier Flugroboter der Fa. Ascending Technologies bezogen um die entwickelte Software Development Platform sowie die Kommunikations- und Mobilitätslösungen im Realsystem zu testen. Zu diesem Zweck wurden zunächst zwei Exemplare des Typs Firefly verwendet, bevor für die abschließenden Tests zwei Exemplare des finalen ANCHORS Fluggeräts bezogen wurden.

Bodenroboter des Typs Jaguar V2 von DrRobot

Die Bodenroboter erweitern die Möglichkeiten des ANCHORS Systems. Mit diesen Robotern ist es möglich die Suche nach radioaktiven Gefahrenstoffen am Boden fortzusetzen, weiterhin bieten sich die Bodenroboter für die Verwendung als Relay-Stationen an, da sie langfristig einsetzbar sind bis die Batterien wieder aufgeladen werden müssen.

Darüber hinaus eignen sich Bodenroboter sehr gut für wissenschaftliche Untersuchungen im Bereich Kommunikation und Mobilität, da die Durchführung von Experimenten leichter ist als vergleichbare Experimente für Flugroboter.

Server für Backend und Simulationen

Die Auswahl von geeigneten Erkundungsstrategien in verschiedenen Szenarien erfolgte unter Zuhilfenahme zahlreicher Simulationsmodelle. Eine Parameteroptimierung wie in Kapitel 5.3 vorgestellt ist nur durch eine hohe Anzahl von Simulationsläufen möglich. Hierfür wurde ein leistungsfähiger Server benötigt.

Mobile Control Stations

Die Flug- und Bodenroboter und die dafür entwickelten Algorithmen wurden in zahlreichen Experimenten validiert. Eine Vielzahl von Experimenten fand dabei auf Segelflugplätzen und großen Ackerflächen statt. Zur Steuerung und Kontrolle des Systems in diesen Bereichen wurden die Mobile Control Stations benötigt.

Embedded Platform

Die embedded Platform wird benötigt um die Software Development Platform und somit die Mobilitätsalgorithmen auszuführen. Jeder Roboter im ANCHORS System verfügt daher über eine embedded Platform.

Software-Lizenzen

Für den Betrieb des Simulationsservers wurde die Software Microsoft Windows Server 2012 Standard benötigt. Hiermit ist der Betrieb von virtuellen Maschinen möglich um eine Vielzahl von parallelen Simulationen laufen lassen zu können.

Ladestationen Akkus

Die beiden finalen Fluggeräte von Ascending Technologies verwenden auch eine neue Akku-Technologie. Für das Laden dieser Akkus wurden Ladestationen beschafft.

LTE Kommunikationssystem

Zur Sicherstellung einer hochzuverlässigen Datenübertragung innerhalb des ANCHORS Systems wurden zwei verschiedene Kommunikationssysteme genutzt: zum einen WLAN Mesh, zum anderen ein eigenständiges LTE Kommunikationssystem. Mithilfe dieser Standalone Lösung ist ein LTE Betrieb unabhängig von einem öffentlichen Mobilfunkanbieter möglich. Diese Unabhängigkeit erhöht die Sicherheit des Systems. In wissenschaftlichen Untersuchungen konnte gezeigt werden wie ein zukünftiger Betrieb eines solchen Systems in öffentlichen Netzen ermöglicht werden könnte.

8. Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die im Rahmen des ANCHORS Projekts von der TU Dortmund durchgeführten Arbeiten waren zwingend notwendig, um die vom Anwender geforderten Aufgaben der nuklearen Erkundung zuverlässig erfüllen zu können. Die entwickelte Schwarmsteuerung erlaubt die Interaktion und Kooperation von verschiedenen Roboterarten und zeigt damit die zukünftigen Möglichkeiten des automatischen Betriebs derartiger Systeme Ein hoch-zuverlässiges Kommunikationssystem unterstützt das Schwarmsystem, indem robust Statusnachrichten ausgetauscht werden können.

Mithilfe einer großangelegten und komplexen Übung konnten die Möglichkeiten des Systems einem breiten Publikum vorgeführt werden. Die Ergebnisse des Projekts konnten auch durch Presse- und TV-Berichterstattung weit über die Community hinaus präsentiert werden.

9. Voraussichtlicher Nutzen, Verwertbarkeit des Ergebnisses im Sinne des Verwertungsplans

Die im Rahmen des ANCHORS Projektes erzielten Ergebnisse werden in Zukunft von der TU Dortmund sowohl in der Bereichen Forschung und Lehre als auch bei zukünftigen Industrieprojekten und Kooperationen eingebracht und verwertet werden. Im Folgenden werden diese einzelnen Bereiche näher erläutert.

9.1 Forschung

In ANCHORS wurden wissenschaftliche Fortschritte insbesondere in den Feldern der Vernetzung unbemannter Roboter, deren kooperativer Betrieb und Erkundung in verschiedenen Einsatzgebieten erzielt. Diese Themenfelder waren zu Beginn des Projekts in großen Teilen noch nicht wissenschaftlich aufgearbeitet, so dass sich ein unmittelbarer Forschungsbedarf identifizieren ließ.

Im Kontext von ANCHORS gab es daher neun wissenschaftliche Fachveröffentlichungen, die auf internationalen Tagungen vorgestellt wurden und mit großem Interesse aufgenommen und diskutiert wurden. Somit konnte der Lehrstuhl einen Beitrag zur Bekanntmachung des ANCHORS Projekts liefern.

Der Lehrstuhl für Kommunikationsnetze organisiert zusammen mit renommierten internationalen Partners, unter anderem dem Aerospace Controls Laboratory des MIT und der University of California, Santa Barbara im Rahmen der international renommierten Konferenz IEEE Globecom den Workshop "Wireless Networking, Control and Positioning for Unmanned Autonomous Vehicles". Der Workshop bietet eine Plattform für die Diskussion der neusten Ergebnisse im Bereich der autonomen Fahrzeuge. Es werden nicht nur MUAVs adressiert, sondern auch autonome Fahrzeuge am Boden, Unterwasser im Weltraum.



9.2 Lehre

Am Lehrstuhl für Kommunikationsnetze finden regelmäßig die Lehrveranstaltungen

- „Kommunikationsnetze“
- „Mobilfunknetze I“
- „Mobilfunknetze II“
- „Betriebswirtschaftliche Grundlagen der IKT“
- „Networked Mobile Robot Systems“

- „Modellbildung und Simulation“
- „Computer Systems“

statt. Die Ergebnisse aus dem ANCHORS Projekt werden in der Zukunft als neue Lehrinhalte mit in die Vorlesungen einfließen. Auf diese Weise werden die Studierenden frühzeitig in konkrete Forschungsthemen eingeführt und erhalten damit einen Überblick des Anwendungsgebietes von Kommunikationsnetzen und Mobilfunknetzen im Speziellen.

10. Bekanntgewordene Fortschritte Dritter

Nachfolgend werden verwandte Vorhaben kurz vorgestellt, welche während der Durchführung des Vorhabens bekannt wurden und sich ebenfalls mit der Verwendung von UAVs für zivile Anwendungen beschäftigen:

Ein Einsatz von luftgestützten Plattformen für *Search and Rescue* (SAR) ist naheliegend und wird daher bereits seit einiger Zeit in verschiedenen Projekten verfolgt. In dem EU-Projekt DARIUS⁷ liegt der Fokus beispielsweise auf der Realisierung einer SAR-Prozesskette für unterschiedliche land- und luftgestützte Plattformen sowie verschiedene Umgebungen (Berg, See, Luft). In dem EU-Projekt AIRBEAM⁸ wurden unterschiedliche Plattformen vom Mikro-UAS bis hin zum Satelliten integriert, um Szenarien der zivilen Sicherheit wie beispielsweise Waldbrände in Südeuropa zu entdecken und zu bekämpfen. Im Bereich der Grenzkontrollunterstützung sind ebenfalls einige Projekte aktiv, wie beispielsweise die EU-Projekte SUNNY, CLOSEYE und AEROCEPTOR⁹.

11. Erfolgte und geplante Veröffentlichungen

- [1] S. Subik, B. Niehöfer and C. Wietfeld. "**Adaptive Multiplexing Gateway for Mission Critical Communications over High Latency IP-based Satellite Backhaul Links**", in: *Proc. of the IEEE International Conference on Technologies for Homeland Security*, Boston, USA, Nov 2012.
- [2] D. Behnke, P.-B. Bök and C. Wietfeld, "**UAV-based Connectivity Maintenance for Borderline Detection**", in: *Proc. of the IEEE 77th Vehicular Technology Conference (VTC-Spring)*, Dresden, Germany, Jun 2013.

⁷ <http://www.darius-fp7.eu/>

⁸ <http://airbeam.eu/>

⁹ www.sunnyproject.eu , www.closeye.eu, www.aeroceptor.eu

- [3] S. Subik, D. Kaulbars, P.-B. Bök and C. Wietfeld. "**Dynamic Link Classification based on Neuronal Networks for QoS enabled Access to Limited Ressources**", in: *Proc. of the 22nd International Conference on Computer Communication Networks (ICCCN), 3rd International Workshop on Context-aware QoS Provisioning and Management for Emerging Networks, Applications and Services (ContextQoS)*, Jul 2013.
- [4] C. Wietfeld. Invited Talk "**Cognitive Networking for Unmanned Aerial Vehicle Swarms**" at *Lehigh University, PA, USA*, Dec 2013.
- [5] S. Subik, P.-B. Bök, D. Kaulbars and C. Wietfeld, "**ADeM: Active Delay Management for Critical Group Communication over Heterogeneous Public Cellular Networks**", in: *Proc. of the IEEE International Conference on Communications 2014 (ICC'14), 1st Workshop Advances in Public Safety and Emergency Communications*, June 2014
- [6] P.-B. Bök, K. S. Kohls, D. Behnke and C. Wietfeld, "**Distributed Flow Permission Inspection for Mission-Critical Communication of Untrusted Autonomous Vehicles**", in: *Proc of the IEEE 80th Vehicular Technology Conference (VTC-Spring)*, Vancouver, Canada, September 2014.
- [7] D. Behnke, N. Goddemeier, J. Möllmer and C. Wietfeld, "**Comparison of Multiobjective Optimization Algorithms for Mobility Behaviors in Autonomous Robot Systems**", in: *Proc. of the IEEE GLOBECOM Workshop on Wireless Networking and Control for Unmanned Autonomous Vehicles (Wi-UAV)*, Dec 2014.
- [8] D. Kaulbars, F. Schweikowski and C. Wietfeld, "**Spatially Distributed Traffic Generation for Stress Testing the Robustness of Mission-Critical Smart Grid Communication**", in: *Proc. of the IEEE GLOBECOM 2015 Workshop on SmartGrid Resilience*, San Diego, USA, Dec. 2015.
- [9] D. Behnke, S. Rohde and C. Wietfeld, "**Design and Experimental Validation of UAV-Assisted Radiological and Nuclear Sensing**", accepted for presentation at *2016 IEEE International Symposium on Technologies for Homeland Security*, Boston, USA, May 2016.