

5G OPPORTUNITY

OPPORTUNITY

Sachbericht zum Verwendungsnachweis im Rahmen des Projektvorhabens

5G-Opportunity – Softwarebasierte 5G Ad-hoc Netzwerke
mit opportunistischer Frequenznutzung

Förderkennzeichen: 19OI22010A, 19OI22010B,
19OI22010C

Teil II: Eingehende Darstellung

Zuwendungsempfänger:	Fraunhofer Gesellschaft e.V. Friedrich-Alexander-Universität Hochschule Bonn/Rhein-Sieg
Durchführende Stelle:	Fraunhofer FIT, Schloss Birlinghoven, St. Augustin Lehrstuhl für Elektrische Smart City Systeme, Nürnberg Hochschule Bonn/Rhein-Sieg, St. Augustin
Projektkoordinator:	Dr. Mathias Kretschmer
Laufzeit:	01.02.2023 – 30.06.2025
Berichtszeitraum:	01.02.2023 – 30.06.2025
Autoren:	Konrad Horbach, Bastian Perner, Willi Rehmann, Mathias Kretschmer

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

1. Anforderungsanalyse

1.1. Szenarien, Technologien und Anforderungen

Der folgende Abschnitt bezieht sich auf die Ergebnisse aus dem Unterpaket AP 1.2 *Anforderungsanalyse aus Nutzersicht (BOS)* und AP6.1

Im Zentrum des Projekts 5G-Opportunity steht die Verbesserung der Kommunikationsinfrastruktur in Notfall- und Katastrophenszenarien. Die Bandbreite an Einsatzszenarien reicht von kurzfristigen und unvorhersehbaren Vorfällen wie Verkehrsunfällen bis hin zu langfristigen Großlagen wie Naturkatastrophen. Die jeweiligen Anforderungen an Kommunikationslösungen variieren dabei erheblich hinsichtlich Planbarkeit, räumlicher Ausdehnung, Anzahl der eingesetzten Endgeräte sowie Dauer und Vorbereitungszeit des Einsatzes. In ad-hoc Situationen wie einem Autobahn-Massenunfall oder einem Zugunglück besteht keine Vorbereitungszeit – hier ist innerhalb weniger Minuten eine zuverlässige Kommunikationsinfrastruktur bereitzustellen. Derartige Szenarien dauern meist einige Stunden bis wenige Tage und erfordern eine kompakte, schnell verfügbare Lösung mit hoher Flexibilität. Bei planbaren Großveranstaltungen wie Musikfestivals hingegen besteht ausreichend Vorlaufzeit. Hier können LuK-Maßnahmen frühzeitig vorbereitet und die notwendige Frequenznutzung lizenziert werden. Obwohl diese Szenarien besser planbar sind, ist auch hier mit starker Netzlast zu rechnen, etwa durch die gleichzeitige Nutzung öffentlicher Netze durch viele Teilnehmer. Auch in diesen Fällen ist eine autonome BOS-Kommunikationslösung von Vorteil. Naturkatastrophen wie Überschwemmungen oder Erdbeben stellen die komplexesten Szenarien dar. Sie treten ohne Vorwarnung auf, betreffen oft große Gebiete und dauern über Wochen an. In solchen Fällen ist ein schneller erster Aufbau einer temporären Infrastruktur essenziell, der dann schrittweise durch eine dauerhaftere Kommunikationsstruktur ersetzt werden kann. Dies erfordert hochgradig skalierbare und robuste Systeme, die auch unter widrigen Bedingungen zuverlässig arbeiten.

Das Kommunikationssystem im Projekt 5G-Opportunity basiert auf einer zweistufigen Netzarchitektur, bestehend aus Zugangs- und Zuführungsnetz. Diese Struktur erlaubt es, lokale Kommunikationseinheiten (z. B. BOS-Leitstellen, Sanitätsstationen, Anlaufstellen für die Bevölkerung) untereinander zu verbinden und mit dem Internet zu koppeln.

Für das Zugangsnetz kommen insbesondere WLAN und 5G in Frage. Während WLAN einfach bereitzustellen ist und von vielen Geräten unterstützt wird, ist die Reichweite begrenzt, sodass für großflächige Abdeckung viele Access Points erforderlich sind. Hier kommt 5G ins Spiel: Das sogenannte Campusfrequenzband im Bereich 3,7–3,8 GHz wird bislang nur in geringem Maße genutzt und bietet daher großes Potenzial für den temporären Einsatz durch BOS. Voraussetzung dafür ist allerdings ein Verfahren zur Erkennung von Primärnutzern (Spektrum-Sensing) und eine entsprechende regulatorische Freigabe.

Das Zuführungsnetz kann auf Richtfunkverbindungen (WLAN-Punkt-zu-Punkt-Strecken), Satellitenverbindungen oder sogar bestehende Infrastruktur wie Glasfaser oder DSL zurückgreifen. WLAN-Richtfunkstrecken bieten eine gute Balance zwischen Verfügbarkeit und Bandbreite, insbesondere da sie in geschützten BOS-Frequenzbändern betrieben werden können. Satellitenverbindungen bieten hingegen nahezu globale Verfügbarkeit, sind aber in ihrer Bandbreite begrenzt und anfällig bei hoher Last.

Durch die Kombination dieser Technologien entsteht ein flexibles, modular aufgebautes Netz, das sich an unterschiedliche Szenarien und Topologien anpassen lässt – ein zentrales Ziel des Projekts 5G-Opportunity.

Die Anforderungen an ein Notfall-Kommunikationsnetz für BOS sind vielfältig und umfassen sowohl technische als auch organisatorische Aspekte.

Ein zentrales Anliegen ist die Verwendung vertrauter Endgeräte. Viele BOS-Mitarbeiter sind ehrenamtlich tätig und verfügen nicht über spezifischen IuK-Hintergrund. Es ist daher nicht praktikabel, für jede neue Technologie eigene Geräte und Schulungen bereitzustellen. Smartphones mit Dual-Connectivity (WLAN und 5G) stellen hier eine praktikable Lösung dar: Sie sind bekannt, flexibel einsetzbar und unterstützen moderne Kommunikationsstandards.

Verfügbarkeit und Robustheit sind ebenfalls entscheidend. Ein solches Netz muss jederzeit einsatzbereit sein, insbesondere bei ad-hoc Ereignissen ohne Vorlaufzeit. Das System soll sich selbst konfigurieren können und wenig manuellen Aufwand erfordern – Self-Organizing Networks (SON) sind hier ein Lösungsansatz.

Ein wesentliches Hindernis ist aktuell die regulatorische Nutzung des 5G-Campusfrequenzbandes. Derzeit ist das Lizenzierungsverfahren langwierig und für BOS nicht praktikabel. Um die Nutzung in Notfällen zu ermöglichen, sind Änderungen im Genehmigungsprozess notwendig, einschließlich automatisierter Verfahren und klar definierter Regeln für ad-hoc Nutzungsszenarien. Eine dynamische Anpassung der Netzkonfiguration in Abhängigkeit von realen Spektrum-Sensing Daten ist hierbei essenziell.

Darüber hinaus ist Interoperabilität wichtig: BOS-Einheiten, freiwillige Organisationen und externe Kräfte müssen in der Lage sein, ihre Geräte und Netzkomponenten in einem gemeinsamen Netzwerk zu betreiben. Dies setzt die Verwendung offener Standards und modularer Komponenten voraus.

Verschiedene Organisationen im Netzwerk benötigen eine logische Trennung. Netzwerk Slicing erlaubt eine virtuelle Aufteilung von Netzwerkressourcen und das Anbieten verschiedener Qualitatesguten (Quality of Service), Priorisierung und Bandbreitengarantien.

1.2. Nutzung des 5G-Campus-Spektrums

Die Frequenznutzung im Bereich von 3,7 bis 3,8 GHz in Deutschland unterliegt strikten regulatorischen Vorgaben. Die Bundesnetzagentur (BNetzA) ist die verantwortliche Behörde, die Lizenzen für die Nutzung dieses Frequenzbandes gemäß dem Telekommunikationsgesetz (TKG) in Verbindung mit der "Verwaltungsvorschrift für Frequenzuteilungen für lokale Frequenznutzungen" erteilt. Das derzeitige Prozedere, das sowohl die Beantragung als auch die Genehmigung umfasst, ist manuell, arbeitsintensiv und zeitaufwändig. Diese Vorgehensweise ist für Hilfsdienste und BOS-Kräfte in ihrer aktuellen Form aufgrund fehlender grundlegender Antragsberechtigung sowie spezieller Anforderungen an das Genehmigungsverfahren nicht praktikabel. Im Laufe des Projekts ist hierzu ein White-Paper entstanden. Das Thema wurde auch eingehend im Abschluss-Workshops mit verschiedenen BOS-Stakeholdern diskutiert. Eine Zusammenfassung des Whitepapers findet sich in Kapitel 5.3.

1.3. User Journey

In diesem Anwendungsbeispiel wird die Planung und Ausführung der Kommunikationsinfrastruktur mit 5G-Campusnetzen durch IuK-Mitarbeiter einer BOS-Einheit in

einem langanhaltenden ad-hoc Katastrophenszenario dargestellt. Nach einer ersten Evaluierung und Sicherung der Lage mit einer temporären Kommunikationsinfrastruktur, wird nun eine Umstellung auf eine längerfristig sichere und stabile Lösung angestrebt.

Diese User Journey stellt die Ziel-Anforderung an den Feldtest dar, in dem das Gesamtsystem erprobt wird (*AP1.4 Evaluationsszenarien für prototypische Entwicklungen*).

Planung

Nach dem Eintritt der Naturkatastrophe werden die LuK-Einsatzkräfte alarmiert und treffen im Zielgebiet ein. Die LuK-Mitarbeiter evaluieren die bestehende Infrastruktur und entscheiden, dass ein Teil des Gebiets mit einem 5G-Campusnetz abgedeckt werden soll. 5G-Funktürme, BOS-Leitstellen, Sanitätsstationen und Leuchttürme sollen über Richtfunkstrecken in ein lokales Telekommunikationsnetzwerk integriert und mit dem Internet verbunden werden.

Aufbau der Netzinfrastruktur

Gegeben durch die geografische Lage und der gewünschten Abdeckung müssen die Funktürme der Richtfunkstrecken positioniert werden. Die Backhaul-Knoten inklusive Antennen werden an diese Funktürme montiert und die Antennen werden ausgerichtet, sodass Sichtverbindung entsteht. Dabei muss der erste Knoten an einem Ort platziert werden, an dem er sich mit dem Internet verbinden kann. Sobald die Knoten mit Strom versorgt werden, baut sich das lokale Telekommunikationsnetz automatisch auf. In Gebieten, die mit einem 5G-Campusnetz ausgeleuchtet werden sollen, werden an den Funktürmen auch noch 5G-Antennen montiert und ausgerichtet und mit dem WiBACK Knoten verbunden. An den Standorten, an denen WLAN-Access angeboten werden sollen, werden die entsprechenden Access-Points auch mit dem Backhaul-Knoten verbunden.

Netzzugang

BOS-Mitarbeiter erhalten Dual-Connectivity Smartphones, welche sowohl 5G- als auch WLAN-fähig sind. Neben 5G wird für die Netzabdeckung an den Sammelstellen WLAN verwendet. WLAN-Zellen decken den unmittelbaren Bereich an festen BOS-Standorten wie Einsatzleitwagen, Sanitätsstation usw. ab. Dabei gibt drei Arten von WLAN Access Point (AP): Offene APs für die Bevölkerung, APs für BOS-Smartphones und APs für alle anderen BOS-Geräte. BOS-Smartphones können sich mit den 5G-Zellen verbinden, die die Bereiche zwischen den WLAN-Zellen abdecken. für die BOS-Smartphones ist ein automatischer Wechsel zwischen 5G und WLAN möglich, je nach der Verfügbarkeit und welche Technologie momentan den besseren Service anbieten kann.

Spektrum-Sensing

Ein BOS-Mitarbeiter bestimmt die Eckpunkte des Gebietes, das mit 5G abgedeckt werden soll. Diese Landmarken werden über eine Nutzerschnittstelle an den Sensing-Controller übergeben. Dies ist an allen Standorten möglich, an denen bereits Netzzugang besteht. Der Sensing-Controller errechnet automatisiert mehrere Positionen an denen 5G-Sensing durchgeführt werden muss. der Mitarbeiter läuft diese Positionen mit einem Sensing-Device ab und übergibt die Messdaten an den Sensing Controller. Auch das kann an allen Punkten erfolgen, an denen

der Netzzugang bereits vorhanden ist. Nun läuft automatisiert die Konfiguration der 5G-Netze. Es wird auf eine Datenbank der Bundesnetz Agentur zugegriffen, um potenzielle Primärnutzer zu ermitteln. Mit den Sensing-Daten und den Informationen von der Bundesnetzagentur wird entschieden, wie die 5G-Zellen konfiguriert werden können. Nach der Entscheidung werden die Ergebnisse der Bundesnetzagentur gemeldet und die 5G-Zellen eingerichtet. Das 5G-Netz kann nun verwendet werden.

Im Betrieb

Die Bevölkerung kann sich mit den offenen Bevölkerungs-APs ohne Passworteingabe verbinden. Ihnen werden die nur die notwendigsten Internetdienste angeboten und deren Datenrate ist derart limitiert, dass sie nicht die Datennutzung der BOS beeinträchtigen. Die BOS-Smartphones authentifizieren sich über die BOS-SIM im WLAN und im 5G-Netzwerk. Dabei sind die Smartphones schon vorkonfiguriert: es gab eine einmalige Einrichtung des 5G-Zugangs (APN-Einstellung) und eine einmalige Einrichtung des WLAN-Zugangs (Auswahl der Authentifizierungsmethode: WPA2/3-Enterprise- EAP-AKA'). Daher ist keine manuelle Eingabe von Passwörtern oder Installation von Zertifikaten erforderlich. Ein BOS-Mitarbeiter, der sich an einem festen BOS-Standort (z.B. ELW) befindet, ist dort mit einem der dortigen WLAN-APs verbunden. Sobald er sich außerhalb der Reichweite des WLAN-APs bewegt, wechselt das BOS-Smartphone auf 5G-Empfang. Beim Eintreten in die Reichweite eines BOS-WLAN-APs erfolgt ein erneuter automatischer Wechsel des Netzwerktraffics von 5G zu WLAN. Es wird noch ein dritter Typ von APs angeboten, an dem sich andere BOS-Geräte mit einem Passwort verbinden können, um auch Geräten ohne SIM-Karten, wie Laptops, einen sicheren Zugang zu dem lokalen BOS-Netz zu ermöglichen.

2. Entwurf und Spezifikation der Architektur

2.1. Gesamtarchitektur

Die Systemarchitektur (Abbildung 1) kann in drei Teile gegliedert werden. Erstens die Komponenten des Zugangsnetzwerks wie gNodeBs für den 5G-Zugang und WLAN-Access Points. Zweitens das Wireless Backhaul-Netzwerk (WBN), das die Zugangszellen mit dem Backbone verbindet. Schließlich gibt es mehrere Controller: Der 5G Core verwaltet die gNodeBs, die Endgeräte und steuert in Kombination mit dem WLAN Authentication Manager den Authentifizierungsprozess. Der selbstorganisierende SDN-basierte WiBACK-Controller verwaltet das WBN. Er wurde erweitert, um Zugangszellen basierend auf den Ergebnissen des Sensing-Controllers zu konfigurieren. Der Sensing-Controller sammelt Messungen, wertet sie aus und berücksichtigt Spektrum Datenbank Abfragen, um verfügbare Kanäle zu erhalten. Für die Kommunikation zwischen dem WiBACK Controller und den Komponenten aus dem Zugangsnetz wurde eine neue Schnittstelle spezifiziert. Der Zugriff auf eine externe Sensing-Datenbank wurde eine bereits spezifizierte Schnittstelle genutzt.

In den folgenden Abschnitten werden die drei Hauptkomponenten und die benötigten Schnittstellen näher beschrieben.

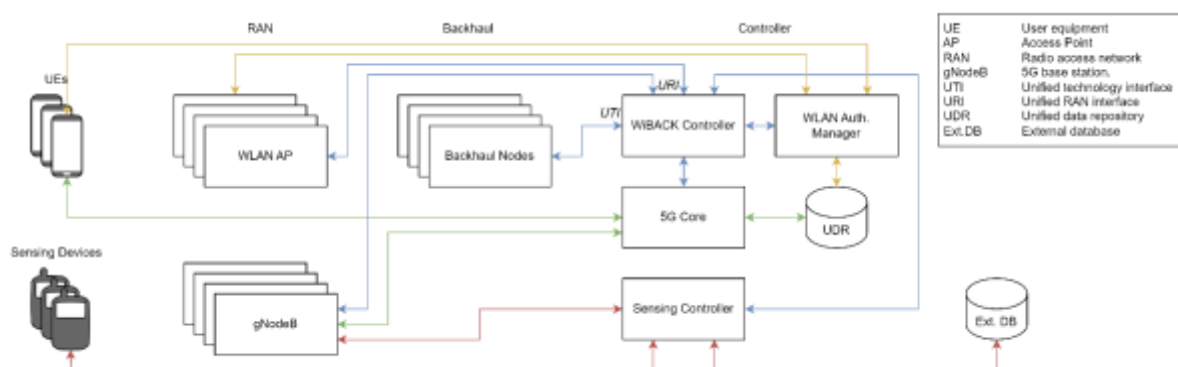


Abbildung 1 Architekturbild

2.2. Wireless Backhaul-Netzwerk

WBN können verteilte Kommunikationsinseln, wie z.B. Leitstellen, Bundeseinrichtungen oder Anlaufstellen für die Öffentlichkeit, mit gerichteten Funkverbindungen verbinden. Da die nächste intakte Backbone-Verbindung weit entfernt sein kann, kann die Internetverbindung über Satellitenverbindungen oder (ggf. mehrere) Funkverbindungen hergestellt werden. Das WiBACK-Framework ist somit technologieunabhängig, die Verbindungen können Ethernet, IEEE 802.11 etc. sein, solange ein entsprechender Technologieadapter implementiert ist. Dank seiner selbstorganisierenden Fähigkeiten erkennt der WiBACK-SDN-Controller die Knoten und fügt sie dem Netzwerk hinzu. Die Backhaul-Links werden automatisch konfiguriert, um die Übertragungsqualität zu verbessern, und der SDN-Ansatz ermöglicht die automatische Zuweisung von Netzwerkkapazität. Diese Plug-and-Play-Funktionen sind besonders für Ersthelfer wertvoll, die sich nicht mit der zeitaufwändigen Netzwerkkonfiguration befassen müssen.

Um die Kommunikation zwischen dem SDN-Controller und den Technologieadaptern zu ermöglichen, definiert WiBACK ein Unified Technology Interface (UTI). Es besteht aus einem minimalen Satz von Primärtypen, um die notwendigen Informationen über die Technologiefähigkeiten und Verbindungsqualitäten zu erhalten und die Backhaul-Verbindung zu konfigurieren. Eine dynamische Frequenzauswahl (Dynamic Frequency Selection, DFS) unterstützt dabei die gemeinsame Nutzung von Funkfrequenzen mit potenziellen Primärnutzern ermöglicht. Zur Konfiguration von Funkzellen wird die Schnittstelle Unified RAN Interface (URI) verwendet.

2.3. Spektrum-Sensing

Spektrum-Sensing ist eine Schlüsseltechnik zur Erstellung eines Lagebildes der aktuellen elektromagnetischen (EM) Situation in einem Zielgebiet. Die Kenntnis der EM-Umgebung bezieht sich in diesem Zusammenhang auf potenzielle Störungen durch legitime Campusnetze, aber auch auf Störungen anderer Quellen wie Störsender. EM-Bewusstsein ist erforderlich, um ein 5G-Campusnetz in einer unbekanntem EM-Umgebung zu betreiben. Die Messungen aller Sensoren werden verwendet, um im Sensing-Controller ein Modell der EM-Umgebung zu erstellen, das in der lokalen Sensor-Datenbank gespeichert wird.

Neben diesen Sensing-Messungen ist eine Datenbankabfrage ein weiterer wichtiger Bestandteil dieses Sensing-Ansatzes. In unserem Ansatz zeigen die Informationen aus der Datenbank jedoch nur das Vorhandensein eines regulären lizenzierten Campusnetzes an. Die Informationen aus der Datenbankabfrage können dann zur Verbesserung des EM-Umgebungsmodells verwendet werden.

Das Modell kann verwendet werden, um zeitlich und räumlich ungenutzte Frequenzressourcen zu finden. Das Modell kann auch zur Quantifizierung und Validierung der Auswirkungen der legitimen Campus-Netze im Einsatzgebiet des eigenen Campusnetzes verwendet werden. Diese Informationen können dann an die externe DB, die beispielsweise von der Bundesnetzagentur betrieben wird, zurückgegeben werden.

2.4. Authentifizierung

Für die Authentifizierung wird in der Gesamtarchitektur ein AAA-Server (Radius) vorgesehen. Dieser hat Zugriff auf die User-Datenbank des 5G-Netzes und kann somit WLAN-Clients, die bereits 5G-Zugang haben, über die SIM-Karte per EAP-SIM oder EAP-AKA authentifizieren.

2.5. Schnittstellenbeschreibung

Unified RAN Interface (URI)

Der WiBACK-Controller nutzt das Unified Technology Interface (UTI), um technologieunabhängig Backhaul-Links zu konfigurieren. Um auch Access-Zellen konfigurieren zu können, wurde im Rahmen dieses Projektes das UTI zu dem Unified RAN Interface (URI) erweitert, um Access Zellen auf gleicher Weise wie Backhaul-Links zu konfigurieren.

Das Ablaufdiagramm in **Abbildung 2** zeigt die einzelnen Schritte die das URI durchläuft um eine Access-Zelle zu konfigurieren. Wenn sich ein WiBACK-Knoten mit einem Access Interface bei dem WiBACK-Controller anmeldet wird die LearnRadioCapabilities Primitive durchgeführt: Der Controller fragt das Interface, welche Eigenschaften das Interface hat. Diese Eigenschaften sind beispielsweise das unterstützte Frequenzband, die maximale Sendeleistung, und verschiedene Modulationen. Im nächste Schritt SpectrumScan werden die verfügbaren Frequenzen ähnlich wie bei Spektrum-Sensing mit externen Geräten gescannt, um Sensing-Daten direkt von der Access-Technologie zu erhalten.

Nachdem ein Kanal ausgewählt worden, prüft das ClearChannelAssesment ob auf dem Kanal wirklich kein Primärnutzer vorhanden ist. Dies ist beispielsweise bei Dynamic Frequency Selection (DFS) im 5 GHz WLAN-Spektrum verpflichtend ist. Nachdem die Zelle dann geöffnet wurde, wird mit In-Service Monitoring sichergestellt, dass man die Zelle direkt schließen kann, wenn ein Primärnutzer entdeckt wird.

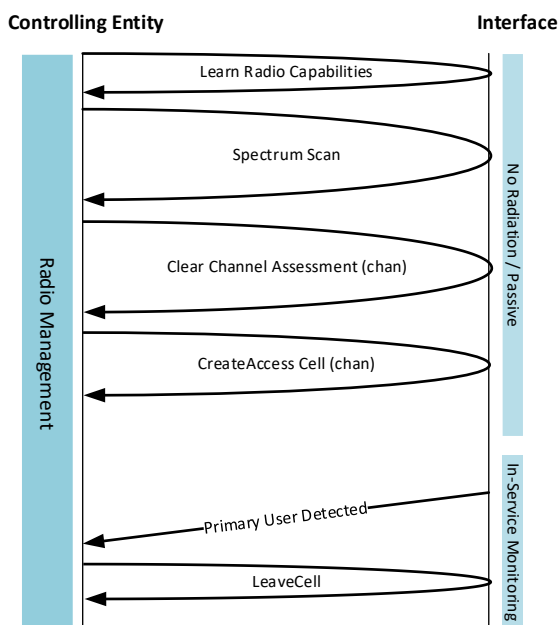


Abbildung 2 Unified RAN Interface (URI)

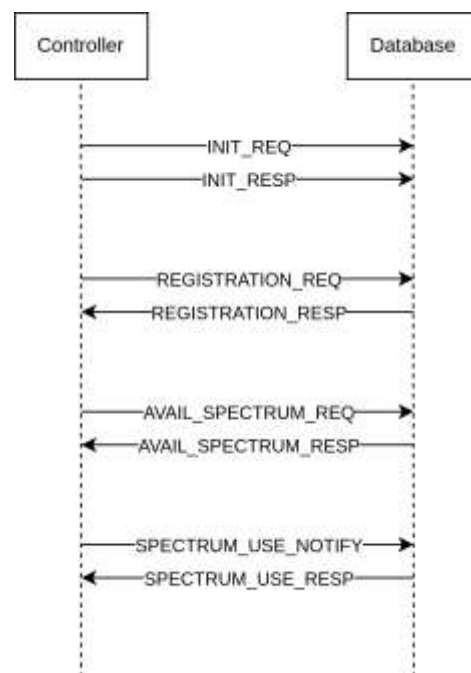


Abbildung 3 Protocol to Access White-Space (PAWS)

RFC 7545 – Protocol to Access White Space (PAWS)

Die durch die Internet Engineering Task Force (IETF) spezifizierte Schnittstelle PAWS kann dazu genutzt werden, um eine zentrale Frequenz-Datenbank abzufragen, ob Spektrum verfügbare ist und genutzt werden darf. Ursprünglich fuer die Nutzung von TV White Space, koennte dieses Protokoll auch fuer die Nutzung von 5G-Campuspektrum genutzt werden. Ein vereinfachtes Ablaufdiagramm ist in **Abbildung 3** zu sehen. Der Sensing-Controller wuerde nach einer Registrierung verfügbares Spektrum abfragen und die Nutzung von Spektrum melden.

3. Entwicklung Zugang

3.1. Network Slicing / Traffic Priorisierung

Um in einem 5G-Netzwerk einzelnen Datenströmen unterschiedliche Bandbreiten zuzuweisen, können unterschiedliche Techniken und Ansätze verwendet werden. Dies hängt stark von der Architektur des Netzwerks und den verwendeten Technologien ab. Im Mobilfunk wird für die Bandbreitenpriorisierung vor allem Quality of Service (QoS) und vereinzelt auch Network Slicing genutzt.

Mit Network Slicing könnte man der BOS einen eigenen Slice mit dedizierten Mobilfunkressourcen geben und hätte die Datenkanäle sauber getrennt. Allerdings lässt sich feststellen, dass der Großteil der aktuell verfügbaren NITB-5G-Systeme kein Slicing unterstützt und auch die Mobiltelefone sich nicht so ohne weiteres an Slices anmelden. Slicing Einstellungen sind vom Betriebssystem nicht direkt zugänglich und müssen über Mobile Device Management Tools konfiguriert werden. Anders als vom Anbieter unseres 5G-Systems (Cocus) beim Kauf in der Projektanfangsphase in Aussicht gestellt, wurde Slicing nicht nachträglich per Update ausgerollt. Um das Problem zu lösen, dass BOS Vorrang zu anderen Netzwerkteilnehmern haben sollen, haben wir uns im Projekt auf das Quality of Service konzentriert.

In einem 5G-Netzwerk spielt Quality of Service (QoS) eine entscheidende Rolle bei der Gewährleistung unterschiedlicher Prioritäten für verschiedene Benutzergruppen. QoS ermöglicht es, bestimmte Traffic-Typen zu priorisieren und ihnen spezifische Bandbreiten zuzuteilen. Die Benutzergruppen werden auf Basis von verschiedenen Kriterien klassifiziert, z.B. durch Identifikatoren wie IMSI, IP-Adresse oder die Art des Dienstes. Innerhalb des 5G-Netzes können spezifische QoS-Klassen (Quality of Service Class Identifiers, QCI) verwendet werden, die den unterschiedlichen Anforderungen der Datenströme gerecht werden. Für eine Benutzergruppe, die Vorrang haben soll (BOS), wurde eine spezielle QoS-Profilierung erstellt und eine garantierte Mindestbandbreite pro Endgerät festgelegt. Die andere Gruppe (Bevölkerung) erhielt eine niedrigere Priorität mit einer dynamischen Bandbreite.

3.2. Spektrum-Sensing

Dieser Abschnitt bezieht sich auf Unterpakete AP3.2 *CRN-Erkennung*, AP3.3 *CRN-Entscheidungsfindung* und AP3.4 *CRN-Datenbank*.

Ein zentraler Aspekt der Aufgabenstellung ist das Spektrum-Sensing, mit dem ein fundiertes Bewusstsein für die EM-Umgebung geschaffen werden soll. Dazu werden verschiedene Informationsquellen genutzt, darunter internes Sensing, externes Spektrum-Sensing und Datenbankabfragen. Der erste Schritt besteht darin, externe Datenbanken abzufragen, um Informationen über potenzielle lokale private Netze in der entsprechenden Region zu sammeln. Anschließend ist externes Spektrum-Sensing durch Personal von Hilfsorganisationen durchzuführen, wobei spezielles Messequipment für die Erfassung von Messwerten – sowohl stationär als auch mobil – eingesetzt wird. Die Messungen können sowohl stationär als auch mobil durchgeführt werden. Wichtig ist dabei eine möglichst gute räumliche Verteilung, um ein

aussagekräftiges Ergebnis zu erhalten. Internes Sensing ist innerhalb des Radio Access Networks (RAN) durchzuführen.

Um das externe Spektrum-Sensing in einem Einsatzfall zu planen, wurden zwei Strategien abgeleitet und implementiert. Damit kann für ein Zielgebiet die Verteilung von einer festen Anzahl an Messpunkten effizient geplant werden. Diese Strategien beruhen auf Optimalitätskriterien aus der sogenannten optimalen Versuchsplanung. Dabei ist das Ziel für die erste Strategie, die auf D-Optimalität beruht, der maximale Informationsgewinn. Die zweite Strategie, basierend auf G-Optimalität, zielt auf ein möglichst robustes Design ab, um auch bei fehlerhaften Messungen ein zuverlässiges Ergebnis zu bekommen. Diese beiden Strategien wurden in einem Konferenzbeitrag hergeleitet und vorgestellt. Darüber hinaus wurden beide Strategien mit Baseline-Strategien verglichen und evaluiert. Die Evaluation basierte auf den Messdaten, die beim Feldtest erhoben wurden.

Nach der Datenerhebung werden die Messdaten verarbeitet. Der Sensing-Controller erstellt ein Modell der EM-Umgebung in der Region und speichert es in einer lokalen Sensing-Datenbank. Mithilfe dieser Informationen können die Auswirkungen des Einsatzes auf andere lizenzierte Campusnetze bewerten werden. Zusätzlich wird auch umgekehrt die Auswirkung von potenziell aktiven primären Campusnetzes auf das eigene zu konfigurierende Netzwerk evaluiert.

Die Daten werden mit einem Interpolationsverfahren verarbeitet und dadurch Radio Environment Maps (REMs) generiert. REMs sind digitale geo-referenzierte Karten, die Informationen über die Funkumgebung enthalten. Beispielsweise kann die enthaltene Information die Signalstärke von Mobilfunknetzen sein. Diese Karte ermöglicht eine detaillierte Analyse der Netzabdeckung und zeigt, in welchen Bereichen der Primäruser aktiv ist. So wurde ein elektromagnetisches Lagebild generiert, mit dem der Einflussbereich des Netzes abgeschätzt und mögliche Abdeckungsgrenzen sichtbar gemacht werden konnten.

Die verarbeiteten Sensing-Ergebnisse werden in der CRN-Datenbank gesammelt. Diese Datenbank bildet somit die lokale Funkumgebung durch REMs ab. Für jeden Kanal wird eine spezifische REM erstellt:

- Signalstärke-REM: basieren auf dem Leistungsdichtespektrum und zeigen die allgemeine Empfangsleistung.
- Netzwerk-spezifische REMs: basieren auf Netzwerk-spezifischen Referenzsignalen (Secondary Synchronization Reference Signal Received Power) und lassen direkt Rückschlüsse auf den Einflussbereich von einzelnen Campusnetzen zu. Damit bilden diese die räumliche Ausbreitung des Netzes ab.
- Modell-basierte REMs: basieren auf Modellen bspw. des eigenen Netzes und sind damit notwendig, um die Ausbreitung des eigenen Netzes abzuschätzen.
- Interferenz-REMs: basieren auf einer Kombination der vorherigen REMs. Diese Interferenz-REMs bilden die Grundlage, um Interferenzszenarien abzubilden und zu identifizieren.

Basierend auf diesen Daten sind Entscheidungen innerhalb des Sensing-Controllers zu optimieren. Mögliche Standorte und Konfigurationen von Basisstationen (BS) werden evaluiert,

indem ihre modellierte Ausbreitung mit den aus Sensing-Ergebnissen gewonnenen REMs abgeglichen werden. Ein Schwellwert-basierter Entscheidungsprozess wird angewendet, um die beste Konfiguration zu identifizieren, ohne dabei die gesetzlichen Richtlinien zu verletzen.

Diese Maßnahmen bilden die Grundlage für die fundierte Entscheidungsfindung und effiziente Planung der CRN-Funktionen. Das erstellte EM-Umgebungsmodell sollte nach Abschluss des Einsatzes auch mit der Bundesnetzagentur geteilt werden.

3.5 Sicherer Zugang / Authentifizierung

Dieser Abschnitt bezieht sich auf Unterpakete AP3.5 *Heterogener COTS Zugang* und AP3.6 *Sicherer Zugang*.

Ein sicherer Netzzugang hängt unabhängig von der Zugangstechnologie von robusten Authentifizierungsmechanismen ab. Passwörter, wie sie in WLANs verwendet werden, dienen der Gruppenauthentifizierung. Alle, die das Passwort kennen, können das Netzwerk nutzen. Eine individuellere und sicherere Methode ist hingegen die Authentifizierung eines einzelnen Nutzers, beispielsweise durch einen Benutzernamen und ein eigenes Passwort. Die Authentifizierung mit einer SIM-Karte ist besonders sicher und gut handhabbar, da der Nutzer dabei keine Daten eingeben muss und die Zugangsberechtigung automatisch über seine eindeutige SIM-Karte erfolgt.

Das Standardisierungsgremium 3GPP hat für 5G zwei Authentifizierungsprotokolle für Authentifizierung über SIM-Karten definiert: 5G-AKA und EAP-AKA (RFC 5448), wobei der Unified Data Management Service des 5G-Kernnetzes (UDM) für die Generierung der AKA-Authentifizierungsvektoren verantwortlich ist. Um WLAN-Clients (Smartphones) zu authentifizieren, die bereits vom 5G-Kern erkannt und im Unified Data Repository (UDR) gespeichert wurden, kann ein Authentifizierungs-, Autorisierungs- und Abrechnungsserver (AAA) entsprechende Authentifizierungsvektoren vom 5G-UDM anfordern und als Authentifizierungschallenge an das Endgerät schicken. Dieser Prozess ermöglicht es PPDR-Nutzern, sich nur mit ihrer (BOS-) SIM-Karte sicher mit dem WLAN-AP einer Hilfsorganisation zu verbinden. Es müssen keine Anmeldedaten manuell eingegeben werden. Sobald ein Smartphone in den WLAN-Einstellungen auf EAP-SIM oder EAP-AKA gestellt ist, kann es sich nahtlos mit jedem AP verbinden, der die BOS SSID ausstrahlt, und bietet über die gegenseitige Authentifizierung einen konsistenten und sicheren Zugang im gesamten Netzwerk. Im Projekt wurde als AAA-Server die Open-Source-Software freeRadius verwendet und als 5G-Kernnetz, das die User-Datenbank enthielt, kam die Software open5GS zum Einsatz.

4. Entwicklung Backhaul

WiBACK wurde erweitert durch Network Slicing und verbesserte Spektrumswahl (konzeptionell) Das Backhaul-Netz zur Vernetzung von einzelnen festen Einsatzbereichen untereinander und an das Internet basiert auf dem vom Fraunhofer FIT entwickelte Netzwerk-Framework WiBACK (wiback.org). Dieses wurde ursprünglich für kosteneffiziente rurale Konnektivität entwickelt. Im Rahmend des Projektes wurde WiBACK an den Anwendungsfall des Katastrophenschutzes angepasst und durch Ende-zu-Ende Network Slicing und CRN-Mechanismen erweitert. Konzeptionell wurde auch die Thematik der Föderation, also das Kombinieren bzw. Zusammenschalten von Equipment mehrerer Akteure zu einem Netz, behandelt.

4.1. Network Slicing

WiBACK wurde so erweitert, dass in einem physikalischen Netz mehrere virtuelle Netze logisch voneinander getrennt werden koennen, damit verschiedene Hilfs-Organisationen, die Bevölkerung und andere das Netz gleichzeitig geschützt nutzen können mit Priorisierung der Einsatzkritischen Applikationen.

Dazu kann man auf der WiBACKs Management Webseite Slices mit den dazugehörigen Netzwerk-Interfaces anlegen und diesen einen relativen Anteil der Gesamt-Ressourcen zuteilen. Das Path Computation Element (PCE) von WiBACK verteilt die Ressourcen gewichtet Max-Min fair.

Die Slices müssen dann noch voneinander Isoliert werden, sodass sie auf die Ressourcen erhalten, die ihnen versprochen worden sind. Dazu wurde ein neues Verfahren basierend auf Random Early Detection (RED) entwickelt, welches in einem Konferenzpapier veröffentlicht wurde.

Der klassische Mechanismus des) wurde dazu entwickelt bei steigender Link Auslastung frühzeitig Pakete zu verwerfen um eine Link-Verstopfung zu vermeiden, Stichwort Congestion Control. In 5G-Opportunity wurde das Konzept so erweitert, dass es die im Network Slicing zugesagten Kapazitäten berücksichtigt. Während RED üblicherweise nur auf die Länge der Warteschlange reagiert, um Verstopfung durch zufälliges Verwerfen von Paketen zu vermeiden, fließt in dieser Variante zusätzlich die versprochene Kapazität eines Slice in die Entscheidung ein. Damit kann jeder Netzknoten eigenständig bestimmen, wann er Pakete eines bestimmten Slice verwerfen muss, ohne dass dafür ein aufwändiges Signalisierungsprotokoll notwendig ist.

Der zentrale WiBACK-Controller berechnet für jeden Slice Pfade und weist ihnen eine garantierte Bandbreite zu. Die Datenpakete dieser Pfade werden dabei mit MPLS-Labels versehen, sodass jeder Knoten sie eindeutig einem Pfad zuordnen kann. Auf Basis dieser Information kennt ein Knoten die zugesagte Kapazität sowie die aktuell genutzte Bandbreite und kann damit lokal die maximale Drop-Wahrscheinlichkeit p_{max} berechnen:

$$p_{max} = \max\left(a \left(\frac{c_{link}}{c_{prom}}\right)^b \left(1 - \frac{c_{prom}}{c_{used}}\right), 0\right)$$

Solange ein Slice weniger als seine zugesagte Kapazität nutzt, werden seine Pakete nicht verworfen. Überschreitet es diese Grenze, wächst die Drop-Wahrscheinlichkeit in Abhängigkeit von der Relation zwischen zugesagter und aktueller Nutzung. Durch das Verändern weiterer Parametern a, b kann zudem gesteuert werden, wie stark Überlastungen abgefangen werden.

Konfigurationsentscheidungen zu berücksichtigen. Mit diesem Wissen kann der Sensing-Controller eine Anfrage an die externe Datenbank stellen, um Informationen über potenzielle Primärnutzer zu erhalten.

Der Technologie-Adapter initiiert anschließend das interne Sensing, eine qualitative Bewertung aller Kanäle anhand mehrerer Metriken, wie der Anzahl empfangener Beacons, des Leistungsspektrums und der Auslastung. Die Ergebnisse werden in derselben Form wie die Messwerte eines Sensing-Gerätes an den Sensing-Controller übermittelt, sodass die Zugriffsschnittstelle wie ein Sensing-Gerät behandelt werden kann. Sobald der Sensing-Controller die Messungen sowohl von den Sensing-Geräten als auch aus dem RAN gesammelt hat, kann er die Daten verarbeiten und dem SDN-Controller eine Liste ungenutzter und qualitativ geeigneter Kanäle für jede Zugriffszelle bereitstellen. Auf Grundlage dieser Informationen kann der Controller für jede Zelle einen Kanal auswählen, wobei systeminterne Interferenzen minimiert werden

Nachdem ein Kanal für eine Zugriffszelle ausgewählt wurde, muss eine „Clear Channel Assessment“ (CCA) durchgeführt werden. Dabei horcht die Netzwerkschnittstelle für eine bestimmte Zeitspanne auf dem gewählten Kanal. Nur wenn in diesem Zeitraum kein Primärnutzer erkannt wurde, darf der Radio-Manager die Nutzung dieses Kanals freigeben. Beispielsweise schreiben die DFS-Regularien eine CCA-Dauer von einer Minute vor. Dieser abschließende Kanalscan schließt die Existenz eines Primärnutzers auf dem ausgewählten Kanal mit Sicherheit aus. Fällt die Antwort negativ aus, das heißt ein Primärnutzer wurde erkannt, wählt der Radio-Manager den nächsten Kanal und initiiert die nächste Clear Channel Assessment, bis diese erfolgreich ist oder kein weiterer Kanal verfügbar bleibt. Eine negative Antwort sollte stets als Hinweis an den Sensing-Controller weitergegeben werden.

Bei einer positiven Clear Channel Assessment kann die Schnittstelle schließlich eine Zelle auf dem entsprechenden Kanal eröffnen. Abhängig von der verwendeten Technologie müssen hierfür spezifische Informationen wie eine Cell-ID oder Sicherheitsdaten bereitgestellt werden. Die Erstellung der Zugriffszelle muss unter Angabe einer geschätzten Nutzungsdauer an die externe Datenbank gemeldet werden. Allerdings sollte das Auslaufen dieser Zeit nicht automatisch den Entzug des Spektrums bedeuten. Die Betreiber des Notfall-Campusnetzes sollten ihre Nutzungsdauer problemlos verlängern können, falls der Notfall länger andauert als erwartet. Kann das Spektrum früher freigegeben werden, wird dies ebenfalls an die externe Datenbank gemeldet.

Ein weiterer Grund für die Freigabe des Spektrums kann die Entdeckung eines anderen (Primär-)Nutzers sein. Während der gesamten Nutzung des ECS muss ein kontinuierliches In-Service-Monitoring durchgeführt werden. Wenn die aktuell genutzten Kanäle belegt werden, muss die betroffene Zelle aufgegeben werden, und das ECS hat schnell zu entscheiden, wie ein Kanalwechsel erfolgen soll. Dazu müssen die Sensordaten erneut ausgewertet und ein neuer Kanal bestimmt werden.

4.3. Interoperabilität durch Föderation

Es wurde ein Konzept zur sicheren Kommunikation in und zwischen 5GOpportunity-Clustern entworfen. Dabei wird angenommen, dass ein 5GOpportunity-Cluster von einem BOS-Anwender betrieben wird. Durch das Hinzufügen von Backhaul-Knoten anderer Anwender

kann das Cluster dynamisch erweitert werden. Hierbei muss sichergestellt sein, dass nur autorisierte Knoten akzeptiert werden. Zusätzlich wurde der Zusammenschluss mehrerer Cluster verschiedener Anwender diskutiert. Im Falle von Föderationen soll den beteiligten Anwendern über Network-Slicing je ein eigenes logisches Netz zur Verfügung gestellt werden. Föderationen sollen erstellt und wieder getrennt werden können.

5. Integration, Evaluierung, Gesamtbewertung

Entgegen dem ursprünglichen Antrag wurde der Feldtest drei Monate vor dem geplanten Zeitpunkt durchgeführt. Grund dafür war die Gelegenheit, den Test auf dem Summer Breeze Open Air Festival, bei dem MHD aktiv ist, durchzuführen. Im Anschluss an den Feldtest erfolgte die Evaluation des Einsatzes. Zum Projektabschluss wurde ein Workshop veranstaltet, in dem eine Mini-Version des Feldtests präsentiert wurde.

5.1. Feldtest

Einsatzszenario



Abbildung 5 Aufbau des Demonstrators auf dem Summer Breeze Open Air

Im Rahmen eines vier Tage andauernden Einsatzes auf dem Summerbreeze 2024 Open-Air Festival (Abbildung 5) bauten die Projektteilnehmer in Zusammenarbeit mit dem Malteser Hilfsdienst die im Projekt entwickelte 5G-Infrastruktur auf und testeten sie unter realen Bedingungen. Das Festivalszenario eignete sich hervorragend für diesen Test, da es die Herausforderungen eines Katastrophenfalls realistisch abbildete – insbesondere die hohe Anzahl

von Menschen auf engem Raum und den damit verbundenen erhöhten Bedarf an sanitären Hilfsleistungen.

Die rund 45.000 Festivalbesucher führten zu einer erheblichen Belastung der kommerziellen Mobilfunkzellen, was erfahrungsgemäß zu Bandbreitenengpässen und Verbindungsabbrüchen führt. Besonders kritisch ist dies für den sanitären Hilfsdienst, dessen Kommunikationsdienste von Netzüberlastungen betroffen sein könnten. Um diesen Herausforderungen zu begegnen, stellten wir den Maltesern eine eigene 5G- und WLAN-Infrastruktur bereit.

An strategisch sinnvollen Standorten wurde eine 5G-Basisstation und WLAN-Access Points installiert, welche per WiBack-Richtfunk miteinander und zum Backhaul verbunden waren.

Spektrum-Sensing für die opportunistische Frequenznutzung

Während des Einsatzes auf dem Festival wurden die Prozesse zur opportunistischen Nutzung des Campusnetz-Frequenzbandes getestet, indem mittels Sensing-Gerät das Spektrum vermessen wurde, um die Nutzung eines Primärusers (Lizenzinhaber eines Campusnetzfrequenzbandes) auszuschließen, bzw. diesen zu detektieren und dessen räumlichen Einflussbereich abzuschätzen und in die Netzwerkplanung einzubeziehen. Da kein Primäruser detektiert wurde, konnten die 5G-Zellen im Campusnetzband N78 (Frequenzbereich 3700-3800 MHz) betrieben werden und gewährleisteten eine zuverlässige und leistungsfähige Verbindung. Nachfolgend wird diese Zelle mit ECS-5G (Emergency Communication System -5G) bezeichnet.

Um dennoch die im Projekt entwickelte Sensing-Technik zu testen, wurde eine zusätzliche 5G-Zelle im südlichen Teil des Festivalgeländes aufgestellt, welche als simulierter Primäruser fungierte und entsprechend vermessen werden sollte. Dafür wurden während des Festivals an verschiedenen Standorten mit dem Netzwerkscanner Rohde & Schwarz TSMA6B Messungen aufgezeichnet. Es wurde die Empfangssignalstärke der Campusnetze mithilfe von SS-RSRP und die spektrale Leistungsdichte aufgenommen. Die Messdaten wurden auch jeweils mit GNSS-Referenzpositionen verknüpft. In Fällen, in denen der Synchronisationsblock (SSB) nicht erkannt wurde, wurde ein Standardwert von -160 dBm zugewiesen. Dies stellt sicher, dass die Daten konsistent bleiben und fehlende Werte einheitlich behandelt wurden.

Die Daten wurden, wie oben beschrieben, zu REMs weiterverarbeitet. Je Kanal und Campusnetz wurde eine Netzwerk-spezifische REM erzeugt. Damit konnte man bereits sehen, dass sich die Abdeckung beider Netze überschneidet. Im Anschluss wurde evaluiert, wie stark sich diese Überschneidung auswirkt, also wie sehr die ad-hoc Zelle das Campusnetz des Primärusers stört. Dazu wurde eine Interferenz-REM erzeugt. In diesem Fall stellt diese Karte die Interferenz zwischen den beiden aktiven Netzwerken, ECS-5G und Primärnutzer, räumlich gesehen, dar. Im Einsatzbereich des Primärnutzers war durchgehend ein Signal-zu-Interferenz Verhältnis von unter 20dB gegeben. Das heißt, das Signal des Primärnutzers ist in diesem Bereich 20dB stärker als das des ECS-5G und somit war keine merkliche Einschränkung des Primärnutzers gegeben.

Bei der Demo des Abschluss-Workshops gab es ein ähnliches Setup. Auf dem Gelände des Schloss Birlinghoven ist bereits ein Campusnetz aktiv. Bei dieser Demo wurde zunächst eine Entscheidung über die Zulässigkeit des Betriebs des ECS-5G getroffen. Es wurde mithilfe eines Spektrum-Sensing Geräts das Spektrum vermessen, vor allem in Bezug auf den Primärnutzer

(das lokale Campusnetz), und erneut eine Signalstärke-REM erzeugt. Darüber hinaus wurde Signalausbreitung des ECS-5G mit einer modell-basierten REM abgebildet.

Legt man nun einen Schwellwert für den zulässigen Störabstand fest, so konnte man eine Entscheidung treffen, ob ein Betrieb in dieser Konfiguration zulässig ist oder nicht. Dabei wurde für zwei beispielhafte Schwellwerte in einem Großteil des Einsatzgebiets der Störabstand nicht eingehalten und somit ist der Betrieb mit dieser Konfiguration nicht zulässig. Die Wahl des Schwellwerts kann von regulatorischen und anwendungsspezifischen Anforderungen abhängen.

Die im Rahmen der Messkampagne erstellten REMs belegen die praktische Anwendbarkeit des opportunistischen Ansatzes. Demnach können Ad-hoc-Netze unter Einhaltung der regulatorischen Vorgaben sowie anderer Einflussfaktoren konfiguriert und betrieben werden. Dafür ist Spektrum-Sensing ein erforderlicher Bestandteil, um einen zuverlässigen zu gewährleisten und auch gemäß der regulatorischen Rahmenbedingungen zu agieren.

Backhaul-Richtverbindung

Es wurde eine umfassende Infrastruktur bereitgestellt. Diese umfasste eine 5G-Basisstation zur Netzabdeckung des In-field-Bereichs (Standort der Hauptbühnen) inkl. einer dort gelegenen Sanitätsstation, sowie die Anbindung an zwei weitere Sanitätsstationen, an denen Outdoor-WLAN-Access-Points installiert wurden. Der ELW steht abseits des Festivalgeländes, verfügt über ein internes Netz und hat einen Internetanschluss. Per WiBACK Richtfunk wurden die Knoten miteinander verbunden und ans interne Netz sowie an das Internet angeschlossen.

Um ein Katastrophen-Szenario mit mehreren Organisationen mit verschiedener Priorisierung darzustellen, wird das Backhaul in vier Slices aufgeteilt. Eine gestimmte Bandbreitenverteilung soll im Falle einer Linküberlastung durchgesetzt werden: Die Malteser sollten 50% des Netzes, 5G und die WLAN-APs jeweils 20% und ein Slice für Privates Surfen 10%.

Der *Malteser Slice* hat die höchste Priorität und den größten Anteil der Bandbreite. Dieser Slice beinhaltet den Datenverkehr, der für die Patientenbetreuung notwendig ist. Dazu wurde in jeder Sanitätsstation ein WLAN-AP mit Passwort eingerichtet. Die Daten die über diese APs in das Backhaul-Netz gelangen in den Malteser Slice. Das interne Netz im ELW ist mit diesem Slice verbunden.

Der *5G Slice* verbindet die gNodeB mit den 5G-Core auf dem Controller. Der *Access Points Slice* beinhaltet die Access Points die SIM Authentifizierung nutzen.

Der *Privates Surfen Slice* soll den Helfern in ihrer Freizeit eine niedrig priorisierte Internetanbindung liefern. Dieser Slice kann die betroffene Bevölkerung in einer Großschadenslage repräsentieren.

Anhand des Durchsatzes des Malteser Slices (**Abbildung 6**) kann man den Verlauf des Festivals sehen. Am Nachmittag haben die Konzerte angefangen und liefen bis in die Nacht. Am Samstag wurde das Netz schon teilweise abgebaut und auf alternativen ausgewichen, um die Abbauarbeiten am Sonntag zu verkürzen. Der Großteil des Datenverkehrs war der Zugriff auf die Leitstellensoftware. Man kann erkennen, dass die Netzwerkverbindung viel genutzt wurde, aber unter 20 Mb/s liegt.

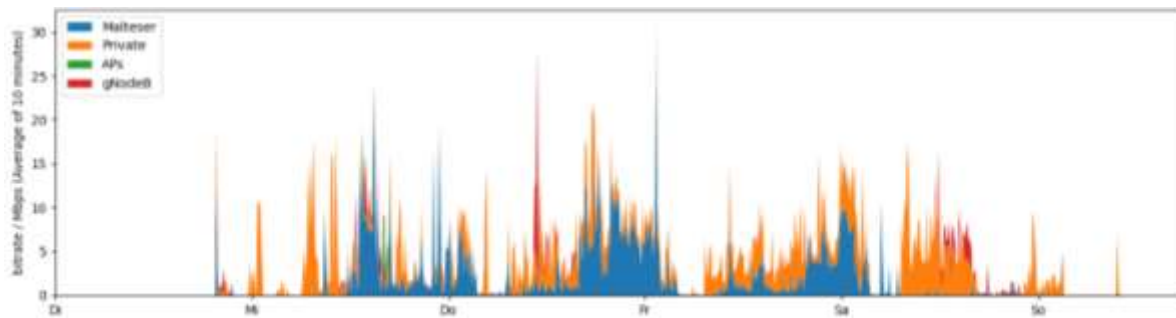


Abbildung 6 Durchsatzmessung im Backhaul-Netz

Der Slice für die gNodeB und die APs wurde nur wenig genutzt. Die 5G-Zelle und die APs mit SIM-Authentifizierung wurden nicht von dem medizinischen Personal genutzt, sondern nur zu Testzwecken. Tests zum Durchsatz und zur Empfangsabdeckung lassen sich in temporären Peaks erkennen.

Der Slice für das private Surfen wurde im Vergleich zu den anderen Slices viel genutzt. Da der Datendurchsatz im Allgemeinen nicht an die physikalischen Grenzen des Netzwerks kommt, kann man keine genauen Aussagen zu der Durchsetzung der Bandbreitenverteilung treffen.

Da WiBACK die WLAN-Technik und entsprechende Frequenzen nutzt, wurde während des Feldtests wurden mehrere 5GHz-WLAN-Scans durchgeführt, bei denen die WiBACK-Knoten die Belegung der Frequenzen passiv erfassten. Es zeigte sich, dass viele SSIDs, hauptsächlich von Festivalveranstaltern und Verkäufern, das Spektrum belegten, einschließlich des für BOS reservierten Bereichs. Daher war der Betrieb des WiBACK-Richtfunks zeitweise geringfügig gestört, da die automatische Regulation der Knoten-Sendeleistungen nicht auf diesen Fall vorbereitet war. Dieses Real-World-Szenario wurde nachträglich in die WiBACK Software aufgenommen, sodass unsachgemäße WLAN-Nutzer dieses Problem nicht wieder hervorrufen sollten.

Passive Signalstärkevermessung mittels Smartphones

Die Malteser-Mitarbeiter erhielten von der H-BRS Smartphones mit angepassten SIM-Karten und konnten für ihre Kommunikation sowohl die bereitgestellten 5G- als auch WLAN-Zellen nutzen. Zehn Malteser-Teams wurden mit Samsung Galaxy A14 Smartphones ausgestattet, die am Körper getragen wurden. Eine Mess-App auf den Smartphones der Malteser und der 5G-Opportunity Mitarbeiter erfasste in regelmäßigen Abständen WLAN- und 5G-Netzwerkparameter, darunter die Empfangssignalstärke und Geo-Daten, und speicherte diese in einer Datenbank. Da sich sowohl die Malteser- als auch die H-BRS-Mitarbeiter während der vier Festivaltage weitläufig bewegten, konnte eine umfangreiche Datensammlung erfolgen. Die gesammelten Daten ermöglichten die Visualisierung der Netzabdeckung und Reichweite der Sendeanlagen auf Karten.

Die 5G-gNodeB des Fraunhofer FIT mit einer Ausgangsleistung von 2×33 dBm und einer Antennenverstärkung von 17 dBi war in der Lage, den Großteil der Festivalfläche mit einer Reichweite von über 1,5 km zu versorgen. Ergänzend führte der Projektpartner FAU ebenfalls Messungen an der 5G-Zelle durch – allerdings mit einem dedizierten Netzwerkscanner von Rohde & Schwarz (TSMA6B). Ein Vergleich der Messergebnisse sollte zeigen, inwiefern COTS-

Smartphones (Commercial Off-The-Shelf) für derartige Vermessungsaufgaben geeignet sind. Hierzu wurde der Empfangspegel RSRP von 2300 Geoelementen (jeweils 0,81 m² groß) verglichen, in denen sowohl die H-BRS als auch die FAU Messungen durchgeführt hatten. Das Ergebnis zeigte, dass der durchschnittliche Messunterschied unter 4 dB lag. Damit konnte bestätigt werden, dass COTS-Smartphones mit entsprechender Mess-App zuverlässig zur Vermessung von 5G-Zellen genutzt werden können, indem sie passiv am Körper getragen werden. Ein wesentlicher Vorteil der Messung mit Smartphones besteht darin, dass das Gelände gleichzeitig mit mehreren Geräten erfasst und überwacht werden kann. Dadurch entfallen aufwendige, eigens organisierte Messfahrten, für die sonst zusätzliches Personal und spezielles Equipment notwendig wären.

5.2. Abschluss-Workshop

Dieser Abschnitt bezieht sich auf Unterpakete AP5.5 und AP6.1

Der Projektabschluss bot eine hervorragende Gelegenheit, die im Projekt erzielten Fortschritte und Ergebnisse in verschiedenen Bereichen in Form eines Workshops zu präsentieren und zu diskutieren. Es wurden Vorträge zu den Themen Anforderungsanalyse, Spektrum-Sensing, Authentifizierung und dem Feldtest beim SBOA gehalten. Diese gaben Einblicke in die erarbeiteten Lösungen. Im Anschluss gab es eine Demonstration, eine Mini-Version des durchgeführten Feldtests, die den Ablauf und die Technologien aufzeigte. Diese Demo bestand aus Spektrum-Sensing sowie Aufbau und Betrieb eines Campusnetzes, wobei sich die Smartphones über die entwickelten Authentifizierungsverfahren im Netz einwählten.

Eine Vielzahl von Teilnehmern war vor Ort, darunter Vertreter von Organisationen wie dem THW, BBK, der RP Kassel, der Hochschule Koblenz, ITUMA, Uniberg, der Feuerwehr Bremen, BNetzA, DRK, FIT, HBRS, MHD und der FAU.

In der Teilnehmerrunde wurden im Anschluss an die Vorträge die zentralen Themen diskutiert. Zum Spektrum-Sensing war dies beispielsweise die Notwendigkeit einer Datenbank zur aktuellen Nutzung des Spektrums erörtert. Ein kritischer Punkt war das Thema Haftung sowie die Verantwortlichkeit für die Verwaltung der Datenbank. Auch die Datenakquise und das Sicherstellen der Korrektheit der Daten wurden intensiv diskutiert. Ferner ging es darum, welche Informationen zwischen den beteiligten Akteuren geteilt werden können und sollten, um eine effiziente und sichere Nutzung des Spektrums zu gewährleisten. Schließlich wurden potenzielle Konzepte für die Bereitstellung des Spektrums speziell für Hilfsdienste erörtert, um deren reibungslosen Betrieb auch in Notfällen sicherzustellen.

Ein weiteres Ergebnis dieser Diskussionen ist die Tatsache, dass dieses Konzept bei den entsprechenden Hilfsdiensten nur auf Akzeptanz trifft, falls die Nutzung im Einsatzfall gesichert ist. Andernfalls wäre dieses System eine Alternative zum aktuellen Equipment, das im Einsatzfall nicht genutzt werden könnte.

5.3. Whitepaper zur Nutzung des 5G-Campuspektrums

Im Folgenden findet sich eine Zusammenfassung eines Projekt-internen Whitepapers, welches im Laufe des Projekts entstanden ist. Hier werden Möglichkeiten der priorisierten

Nutzung durch BOS Kräfte diskutiert. Die Kernaussagen wurden auch im Workshop (Abschnitt 5.2) diskutiert. Hier sei noch einmal auf den letzten Abschnitt aus 5.2 verwiesen: "...dass dieses Konzept bei den entsprechenden Hilfsdiensten nur auf Akzeptanz trifft, falls die Nutzung im Einsatzfall gesichert ist." Dies bedeutet, dass auf politisch/regulatorischer Ebene eine Lösung gefunden werden muss, die den BOS in einer Schadenslage die (priorisierte) Nutzung von entsprechendem Spektrum zusichert.

Um das Spektrum für Hilfsorganisationen und BOS-Kräfte nutzbar zu machen, muss zunächst eine grundsätzliche Nutzungserlaubnis regulatorisch ermöglicht werden. Die Bedingungen und das Ausmaß der Nutzung sowie die Gestaltung entsprechender Verfahren sind in einem kooperativen Prozess zwischen den beteiligten Interessensgruppen zu klären. Eine allgemeine Nutzungsgenehmigung wäre aus Sicht der Hilfsorganisationen ideal, muss aber die Interessen aller Beteiligten berücksichtigen, um eine übermäßige Einschränkung zu vermeiden, die das Potenzial der industriell genutzten Campusnetze schmälern könnte.

Abhängig von den spezifischen Einsatzszenarien könnten verschiedene Genehmigungsverfahren erforderlich sein, um eine flexible und schnelle Reaktion in Notfallsituationen zu gewährleisten: Das Planungs- und Genehmigungsverfahren sollte für langfristig planbare Ereignisse die Bedarfe aller Interessensgruppen sorgfältig abwägen und berücksichtigen. Beispielsweise haben Veranstalter von Großereignissen einen berechtigten Bedarf, das Spektrum für Campusnetze für Zwecke der Veranstaltungsdurchführung nutzen zu können. Der Spektrumsbedarf der Hilfsorganisationen ist im Normalbetrieb der Veranstaltung dann auch vergleichsweise gering. Jedoch ist es erforderlich, im Falle einer Schadenslage das vorhandene Spektrum dynamisch anzupassen und die Erfordernisse der Einsatzkräfte bestmöglich zu erfüllen. Hierbei könnten z.B. Pläne und Prozesse zum Tragen kommen, die vorab durch die Landkreise als unterste Katastrophenschutzbehörden genehmigt wurden. Technisch realisierbar wäre dies z.B. durch unterschiedliche Prioritäten der einzelnen Netzteilnehmer.

Ad-hoc-Einsätze sind zunächst von einer beginnenden Phase großer Unsicherheiten geprägt. Je nach Schadensumfang dauert diese Phase kürzer oder länger und ist schwächer oder stärker ausgeprägt. In solchen Einsätzen muss die Genehmigung zur Nutzung des Spektrums durch vollständig automatisierte Prozesse und Abläufe erfolgen. Kapazitäten, die Spektrumsnutzung anzumelden oder gar zu beantragen, bestehen nicht. Die Dokumentation der Nutzung kann, wie in anderen Anwendungsszenarien bereits praktiziert, ggf. nachträglich erfolgen, sofern dies als geboten erscheint. Sofern kein Interessenskonflikt prognostiziert wird, sind auch Komplikationen während der Einsatzdurchführung unwahrscheinlich. Nichtsdestotrotz sollte eine begleitende Spektrumsmessung (Sensing) parallel zu jedem Einsatz erfolgen. Der gesicherte Betrieb von Behördenkommunikation kann auf diesem Wege sichergestellt werden. Die gewonnenen Daten sollen als Basis der eigenen Netzoptimierung, im Zweifelsfall aber auch als Grundlage für eine Rückmeldung an die BNetzA hinsichtlich der eigenen und fremden Nutzung des Spektrums dienen.

Werden bereits im Vorfeld beim Abgleich des Einsatzortes mit vorhandenen Campusnetzen mögliche Konflikte festgestellt, sind eine Reihe von Optionen denkbar. Ein Sensing ist in allen Fällen unerlässlich. Sollte das verfügbare Spektrum zwischen 3,7 und 3,8 GHz nicht vollständig genutzt sein, gilt es, die bei der BNetzA angemeldeten Werte durch ein Sensing zu verifizieren. Den Einsatzkräften verbliebe dann die Nutzung des übrigen Spektrumbereiches im ungenutzten Teil. Sofern das Spektrum im Bereich 3,7 bis 3,8 GHz vollständig genutzt ist, sind mehrere Optionen denkbar. Bei bereits vorhandenen Campusnetzen könnten diese koexistierend

betrieben werden. Der Mobilfunkstandard 5G ist prinzipiell für die Koexistenz mehrerer Zellen im gleichen Frequenzband geschaffen. Eine andere Option wäre, den betroffenen Dritten einen Teil des Spektrums temporär abzuerkennen und für die Nutzung zu versagen. Dies technisch automatisiert umzusetzen ist jedoch mit erheblichem Aufwand verbunden. Ebenso könnten, je nach Bedingungen der Zuteilung, Schadenersatzansprüche entstehen.

In solchen Szenarien wäre es denkbar, bereits bei der Zuteilung zwischen kritischen (z.B. Campusnetze im Gesundheitswesen oder der Prozessindustrie) und nicht-kritischen Campusnetzen (verbleibende Wirtschaft) zu unterscheiden. Regulatorisch könnte ein Teil des Campusnetzspektrums (z.B. die unteren 20 MHz) bevorzugt für die ad-hoc Nutzung durch die BOS zugeteilt werden. Somit könnte dies in der Planungsphase von Campusnetzen berücksichtigt werden.

6. Publikationsliste

Im Rahmen des Projektes wurden mehrere Publikationen zur Verbreitung dessen Projektinhalte und wissenschaftlichen Ergebnisse veröffentlicht. Diese sind in der nachfolgenden Liste dargestellt. In der Veröffentlichung *Opportunistic 5G Spectrum Usage for Nomadic Ad-Hoc Emergency Communication* wurde das Gesamtkonzept des Projektes vorgestellt.

- K. Horbach and M. Kretschmer, "A Random Early Detection Approach for Capacity Policing in Wireless Backhaul Networks", Konferenz-Papier, 2024 International Conference on Smart Applications, Communications and Networking (SmartNets)
- K. Horbach, B. Perner, W. Rehmann, M. Kretschmer, M. Luebke, M. Rademacher, N. Franchi, "Opportunistic 5G Spectrum Usage for Nomadic Ad-Hoc Emergency Communication", Konferenz-Papier, 2024 IEEE Future Networks World Forum (FNWF)
- B. Perner, M. Luebke, N. Franchi, "Optimized Measurement Location Planning for Interpolation-based Radio Environment Maps", Konferenz-Papier, 2025 European Signal Processing Conference (EUSIPCO)
- K. Horbach, R. Schmidt, B. Perner, M. Rademacher, „Autarke Breitbandnetze im Katastrophenfall – Forschung auf dem Summer Breeze Open Air“, Artikel in Crisis Prevention, dem Fachmagazin für Gefahrenabwehr, Innere Sicherheit und Katastrophenhilfe, Ausgabe 3/2025