Zuverlässige Kommunikations- und Authentifizierungstechnologien für den BVLOS-Einsatz von Drohnen

Christian Reil, M.Eng.
Patrick Purucker, M.Sc.
Nicholas Jäger, M.Sc.
Prof. Dr.-Ing. Alfred Höß
Prof. Dr. Andreas Aßmuth

Zusammenfassung

Mit dem Forschungsprojekt ADACORSA (https://www.adacorsa.eu/) hat sich die EU zum Ziel gesetzt, die Entwicklung und den Einsatz von unbemannten Drohnen, die außerhalb der Sichtweite des Bedieners operieren, zu stärken. Dazu sollen die notwendigen technischen Komponenten erforscht und entwickelt werden. Die Ostbayerische Technische Hochschule Amberg-Weiden (OTH AW) trägt hierzu im Bereich der sicheren und zuverlässigen Kommunikation bei. Ein von ihr entwickeltes flugfähiges Messsystem dient der Erfassung der Verbindungsqualität von Mobilfunkverbindungen bei Drohnenflügen. Die damit erhobenen Messdaten dienen sowohl als Grundlage für die Entwicklung einer Echtzeitvorhersage der Verbindungsqualität als auch einer verbindungsqualitätsbasierten Flugroutenplanung. Ferner wurde ein Authentifizierungs- und Vertrauensmanagementsystem für Netzwerke von Drohnen auf Basis einer dezentralen Infrastruktur entwickelt.

Abstract

With the ADACORSA research project (https://www.adacorsa.eu/), the EU has set the goal of promoting the development and use of unmanned drones that operate beyond the operator's line of sight. To this end, the necessary technical components are to be researched and developed. The University of Applied Sciences Amberg-Weiden is contributing to the common goal with safe and reliable communication. A flight-capable measuring system developed by the university is used to record the quality of mobile network connections during drone flights. The collected measurement data serve as the basis for the development of both a real-time prediction of the connection quality and a flight route planning based on the connection quality. Furthermore, based on a decentralised infrastructure, an authentication and trust management system for drone networks is developed.

1 Einleitung

Unbemannte Luftfahrzeuge (UAVs – Unmanned Aerial Vehicles), oft auch einfach Drohnen genannt, halten in immer mehr zivilen Bereichen Einzug. Seien es Hobbyanwendungen, z. B. zum Erstellen von Videoaufnahmen, oder kommerzielle Anwendungen, wie z. B. bei Inspektionsaufgaben. Obwohl UAVs, die in Sichtweite eines Drohnenpiloten betrieben werden, bereits viele Einsatzszenarien abdecken können, kann das volle Potenzial dieser Technologie erst durch UAVs, die BVLOS (Beyond Visual Line of Sight, außerhalb der Sichtweite) operieren, ausgeschöpft werden, wofür jedoch erst die technischen und regulatorischen Voraussetzungen geschaffen werden müssen.

Das im Jahr 2020 gestartete und von der EU und nationalen Behörden geförderte Forschungsprojekt ADACORSA („Airborne Data Collection on Resilient System Architectures“) hat sich zum Ziel gesetzt, technische und regulatorische Komponenten für den BVLOS-Einsatz von zivilen Drohnen zu entwickeln, um eine Adaption innerhalb der EU voranzutreiben [1]. Der BVLOS-Betrieb erfordert neben angepassten regulatorischen Anforderungen einen hohen Grad an Autonomie der Drohne. Unter anderem durch den Transfer von Technologien aus dem Automobilsektor sollen technologische Entwicklungen aus dem Bereich des autonomen Fahrens genutzt werden. Im Rahmen von ADACORSA leistet die OTH AW als Partner in

der Supply Chain 4 einen Beitrag zur Sicherheit, Zuverlässigkeit und Effizienz der Kommunikation zwischen BVLOS-operierenden Drohnen untereinander und mit der Bodenstation [2].

Konkret beschäftigt sich die OTH AW zum einen mit der vertrauensbasierten Sicherheit in Flying Ad-hoc Networks (FANETs). Dazu wird im Abschnitt 5 auf die Authentifizierungstechnologien in Netzwerken von Drohnen eingegangen und ein von der OTH AW entwickelter Ansatz zum dezentralen Management der Vertrauensbeziehungen zwischen den Drohnen vorgestellt. Neben dem Thema Sicherheit spielt bei BVLOS-operierenden Drohnen die Kommunikation mit der Bodenstation bzw. dem Operator eine wichtige Rolle. Die OTH AW beschäftigt sich daher zum anderen mit der Zuverlässigkeit von Mobilfunkverbindungen für den Drohneneinsatz. Dazu wurden Vorhersagemodelle für die Verbindungsqualität (QoS – Quality of Service) des LTE- und 5G-Mobilfunks entwickelt, welche sowohl zur Flugroutenplanung (Abschnitt 3) als auch zur Echtzeitvorhersage des QoS während des Fluges (Abschnitt 4) eingesetzt werden können. Grundlage für die Entwicklung dieser Modelle bilden vorangegangene Messungen des QoS, was in Abschnitt 2 beschrieben wird.

2 QoS-Messungen

Zur Erfassung und Aufzeichnung der Verbindungsqualität von Mobilfunkverbindungen während des Drohnenfluges wurde ein In-Flight-Messsystem entwickelt. Die Hauptkomponenten des Messsystems sind ein Einplatinencomputer (Raspberry Pi 4) als zentrale Rechenplattform und zwei baugleiche 5G Modems, welche die gleichzeitige Messung der Verbindungsqualität von zwei verschiedenen Mobilfunkanbietern ermöglichen. Die Messhardware wurde in ein Gehäuse verbaut, mit Antennen bestückt und an einer handelsüblichen Drohne montiert. Das fertige System ist in Abbildung 1 dargestellt. Das Messsystem erfasst zum einen physikalische Signalparameter, welche aus den Mobilfunkmodems ausgelesen werden, darunter verschiedene Messgrößen zur Signalstärke und zum Signal-Rausch-Verhältnis. Insgesamt werden so ca. 200 Parameter pro Modem mit einer Updaterate von 2 Hz aufgezeichnet. Zum anderen werden Parameter bezüglich des QoS der Datenübertragung auf UDP-Protokollebene erfasst. Neben der Messung des Datendurchsatzes und der Paketverlustrate wird auch die unidirektionale Latenz (One-Way-Latency) gemessen. Darüber hinaus werden der Flugzustand und die GPS-Position aufgezeichnet.

Umfangreiche Messkampagnen wurden an verschiedenen, im ländlichen Raum gelegenen, Standorten durchgeführt. Zur Datenerhebung wurde der Luftraum bis zu einer Höhe von 120 m über dem Boden in einem dreidimensionalen Raster mit vorher festgelegten Wegpunkten abgeflogen. Der Flug erfolgte immer in Sichtweite zur Drohne. Die Messungen wurden mehrmals an verschiedenen Tagen und Uhrzeiten und auch mit unterschiedlichen Geschwindigkeiten wiederholt, um eine umfangreiche Datenbasis zu erhalten und einer Verzerrung der Daten entgegenzuwirken. Die aufgezeichneten Datensätze dienten dann als Grundlage für die Entwicklung der im Folgenden beschriebenen QoS-Vorhersage und Flugroutenplanung.

Abbildung 1: In-Flight-QoS-Messsystem, montiert auf eine handelsübliche Drohne.

3 QoS-basierte Flugroutenplanung

Aufbauend auf den erhobenen QoS-Messdatensätzen sollte eine ortsbasierte QoS-Flugroutenplanung demonstriert werden, die sowohl vor als auch während der Flugmission eingesetzt werden kann. Aufgabenspezifische Anforderungen an die Kommunikationsverbindung zur Drohne, z. B. dem Command and Control (C2) Link, sollen so bei der Flugplanung berücksichtigt werden können. Grundlage für die Routenplanung sind sogenannte Konnektivitätskarten, welche aus den Datensätzen generiert wurden. Zur Erstellung dieser Karten wurden die im Luftraum verstreut gemessenen Daten zunächst mithilfe der Gauß-Prozess-Regression (GPR), die auf einem geostatistischen Modell basiert, auf ein dreidimensionales gleichmäßiges Gitter interpoliert. Anschließend erfolgte eine Zusammenführung der einzelnen Messflüge (u. a. durch Mittelwertbildung).

Auf Basis der erstellten Konnektivitätskarten wurde ein auf der A*-Suche ([3]) basierender Pfadplanungsalgorithmus implementiert. Dieser Algorithmus berechnet den kürzesten Weg von einem Startpunkt zu einem Zielpunkt unter Gewichtung verschiedener vom Benutzer vorgegebenen Anforderungen, wie z. B. der Sicherstellung einer definierten Mindestdatenrate oder einer maximalen Latenzzeit. Durch den Einsatz von Multi-Link-Kommunikation besteht die Möglichkeit, die Karten verschiedener Mobilfunkprovider zu kombinieren, um Versorgungslücken einzelner Anbieter zu vermeiden und mehr Möglichkeiten für die Suche nach einem effizienten Pfad zu haben. Abbildung 2 zeigt die grafische Oberfläche der QoS-basierten Flugplanung inklusive der Darstellung des berechneten QoS-optimierten Pfades, die zu

Demonstrationszwecken erstellt wurde. Anzumerken ist, dass dieser Ansatz der QoS-abhängigen Flugplanung auf Gebiete begrenzt ist, in denen ausreichend Messdaten zur Verfügung stehen. Auch müssen für einen realen Einsatz dieser Pfadberechnung Änderung und Abhängigkeiten der Gegebenheiten, z. B. durch Netzausbau, berücksichtigt werden.

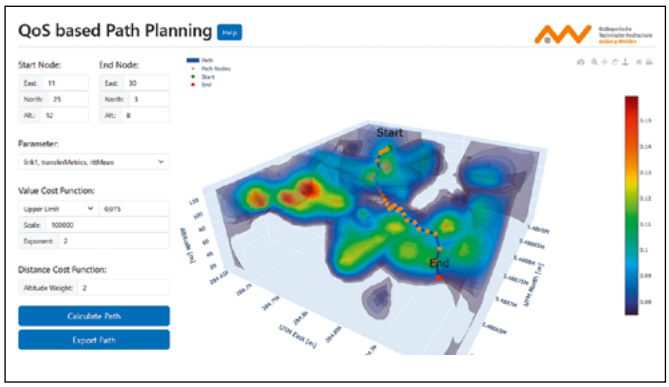

Abbildung 2: Benutzeroberfläche der QoS-basierten Flugroutenplanung.

4 Vorhersage des QoS

Um die Zuverlässigkeit der Verbindung zwischen UAV und Operator zu erhöhen, werden in einem sogenannten Multi-Link Communication Gateway mehrere redundante Verbindungen verwendet. Um die Kanalkapazität der einzelnen Verbindungen nicht zu überlasten und die zu übertragenden Daten entsprechend zu verteilen, wird ein Vorhersagemodell für den QoS der Verbindungen entwickelt. Dabei liegt der Fokus auf der Vorhersage des QoS für komplexe Netzstrukturen wie dem Mobilfunk. Anders als bei direkten Verbindungen, bei denen die Pfadverluste in Abhängigkeit von der Entfernung zum Sender mittels Funktionen modelliert werden können, wirken beim Mobilfunk mehrere Faktoren, wie beispielsweise der Einfluss der Nachbarzellen. Zusätzlich können bei mobilfunkbasierten Verbindungen beim Handover zwischen zwei Mobilfunkbasisstationen Latenzspitzen auftreten. Darüber hinaus kommt es im UAV-Kontext zu einer Verschlechterung des QoS mit zunehmender Flughöhe [4]. Um diese Schwankungen vorhersagen und gegebenenfalls Gegenmaßnahmen einleiten zu können, werden KI-basierte QoS-Vorhersagemodelle entwickelt und evaluiert.

Das Modell, das auch auf einer Edge-Plattform auf dem UAV ausgeführt werden soll, basiert auf der Architektur von Long-Short-Term Memory (LSTM). Dabei wird anhand des Verlaufs von Signalparametern und Paketcharakteristika eine zeitliche Vorhersage für die Latenz berechnet. Der Entwurf des Modells unterstützt die Ausführung auf leichtgewichtiger und stromsparender Hardware. Die verwendete Hardware wird in Abbildung 3 gezeigt. Hierbei findet die Vorverarbeitung auf der CPU des NXP LS1012A (grün) statt, während die Ausführung des Modells auf dem Intel Neural Compute Stick 2 (blau) erfolgt.

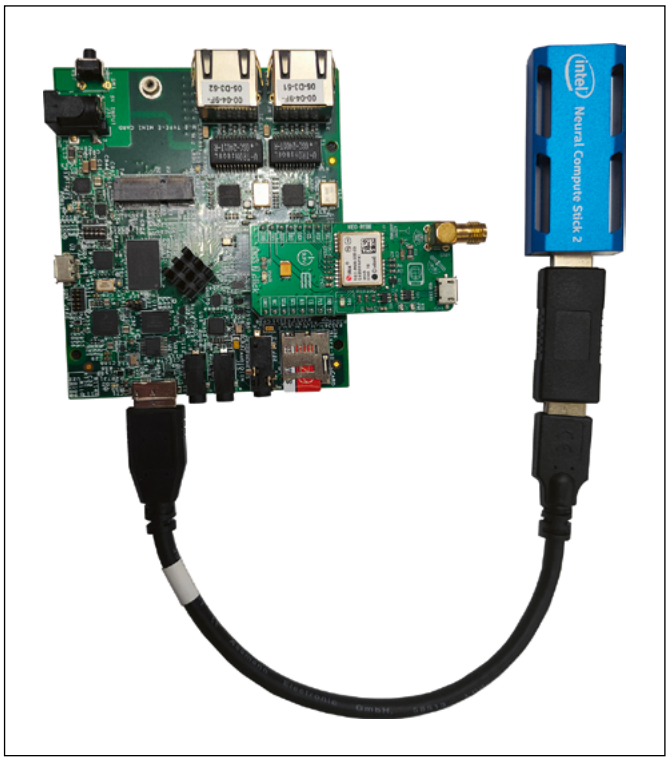

Abbildung 3: Integrierte Hardware, bestehend aus NXP-Board, GPS-Modul und Intel Neural Compute Stick 2.

5 Authentifizierungstechnologien in Netzwerken von Drohnen

Zivile Drohnen, die (semi-)autonom außerhalb der Sichtverbindung operieren, verfügen über ein großes Anwendungspotenzial und benötigen daher entsprechende IT-Sicherheitsmaßnahmen, um eine sichere Anwendung und Schutz vor Angriffen zu gewährleisten. Authentifizierungstechnologien ermöglichen die sichere Verifizierung des Kommunikationspartners, wodurch sichere Kommunikationsverbindungen aufgebaut und Rechte gewährt werden können. Dieser Beitrag behandelt die Authentifikation in offenen Netzwerken von Drohnen. D. h. es wird die Authentifizierung von Drohnen untereinander und nicht beispielsweise die Authentifizierung von Operatoren besprochen.

In offenen Netzen werden Public-Key-Infrastrukturen als Authentifizierungstechnologie verwendet. Public-Key-Infrastrukturen erlauben die Verwendung von Public-Key-Kryptografie, indem digitale Zertifikate verwendet werden, die öffentliche Schlüssel mit Personen oder Gegenständen verknüpfen. Die Verknüpfung basiert dabei auf Vertrauensbeziehungen, welche durch ein Vertrauensmodell geregelt werden. Vielfach werden hierarchische Public-Key-Infrastrukturen verwendet, welche auf hierarchischen Vertrauensmodellen basieren: Nur Zertifizierungsstellen haben das Recht, Zertifikate an Nutzer oder andere untergeordnete Zertifizierungsstellen auszustellen und diese wieder zurückzurufen. Zertifizierungsstellen als zentrale Stellen sind attraktive Angriffsziele und stellen Fehlerquellen dar, wodurch eine Überwachung der

Zertifizierungsstellen notwendig wird, welche wiederum durch zentrale Stellen erfolgt. Dezentrale Public-Key-Infrastrukturen stellen dazu Alternativen dar. In den entsprechenden dezentralen Vertrauensmodellen dürfen die Teilnehmer sich gegenseitig Zertifikate ausstellen und müssen darüber entscheiden, ob sie Zertifikaten von anderen Teilnehmern vertrauen. Dadurch können mithilfe von gemeinsamen Bekannten andere Teilnehmer authentifiziert werden.

Im Rahmen des ADACORSA-Projekts wurde eine dezentrale Blockchain-basierte Public-Key-Infrastruktur für Drohnen entwickelt [5]. In einer speziellen Blockchain können die Nutzer ihre Identität und ihren öffentlichen Schlüssel sowie ihre Vertrauensbeziehungen speichern, wodurch Zertifikate ersetzt werden. Die Vertrauensbeziehungen können mathematisch als Graph, dem sogenannten Vertrauensgraph, modelliert werden. Es wird ein einfaches Vertrauensmodell verwendet: Die Nutzer geben an, wie weit ein anderer Nutzer im Graph maximal entfernt sein darf. Eine Entfernung von zwei würde beispielsweise bedeuten, dass man seinem Nachbarn und dessen Nachbarn vertraut. Die in der Blockchain gespeicherten Daten sind dabei vor Veränderungen geschützt und für alle zugänglich, d. h. für alle überprüfbar. Die Drohnen können während eines Einsatzes, wenn sie eine Verbindung zum Blockchain-Netzwerk haben, sich mithilfe der Blockchain gegenseitig authentifizieren. Alternativ können sie auch den für sie relevanten Teil des Vertrauensgraphen speichern und diesen im Falle, dass sie keine Verbindung zum Blockchain-Netzwerk haben, nutzen. In Abbildung 4 ist das Konzept schematisch dargestellt.

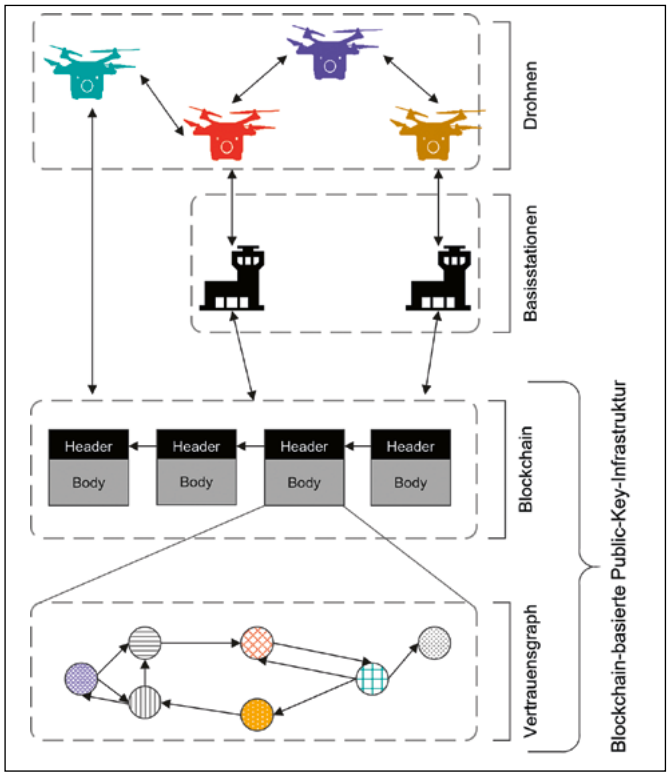

Abbildung 4: Konzeption einer Blockchain-basierten Public-Key-Infrastruktur.

6 Zusammenfassung

Im Rahmen des EU Forschungsprojektes ADACORSA konnte die OTH AW einen Beitrag zur Stärkung der Entwicklung und des Einsatzes von BVLOS-operierenden Drohnen innerhalb der EU leisten. Ein entwickeltes Messsystem ermöglicht es, die Verbindungsqualität von Mobilfunkverbindungen während des Drohnenflugs zu messen. Umfangreiche Datensätze mit einer Vielzahl von für die Verbindungsqualität relevanten Parametern konnten so generiert werden. Zum einen wurde mit diesen Datensätzen die verbindungsqualitätsbasierte Flugroutenplanung demonstriert, indem dreidimensionale Konnektivitätskarten erstellt wurden. Zum anderen dienten diese Datensätze zum Training von auf neuronalen Netzen basierenden Modellen, welche eine zeitliche Vorhersage der Verbindungsqualität ermöglichen. Ebenfalls wurde von der OTH AW das Thema Sicherheit in Kommunikationsnetzwerken von Drohnen behandelt und in diesem Kontext eine dezentrale Blockchain-basierte Public-Key-Infrastruktur entwickelt, welche für das Vertrauensmanagement zwischen Drohnen eingesetzt werden kann.

Referenzen:

[1] „ADACORSA Webseite,“ [Online]. Verfügbar unter: https://adacorsa.eu/.

[2] N. Jäger, P. Purucker, C. Reil, A. Höß, und A. Aßmuth, “Forschungsprojekt: ADACORSA ‘Airborne data collection on resilient system architectures”, Forschungsbericht 2021, p. 6, 2021.

[3] L. Yang, J. Qi, J. Xiao und X. Yong, “A literature review of UAV 3D path planning”, Proceedings of the World Congress on Intelligent Control and Automation (WCICA), vol. 2015, pp. 2376–2381, Mar. 2015, doi: 10.1109/WCICA.2014.7053093.

[4] P. Purucker, J. Schmid, A. Höß, und B. W. Schuller, ‘System Requirements Specification for Unmanned Aerial Vehicle (UAV) to Server Communication’, in 2021 *International Conference on Unmanned Aircraft Systems (ICUAS)*, Athens, Greece: IEEE, Jun. 2021, pp. 1499–1508. doi: 10.1109/ICUAS51884.2021.9476799.

[5] N. Jäger und A. Aßmuth, “An Approach for Decentralized Authentication in Networks of UAVs”, CLOUD COMPUTING 2021 : The Twelfth International Conference on Cloud Computing, GRIDs and Virtualization, S. 13-17, 2021.

Fördergeber:

ADACORSA has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876019. The JU receives support from the European Union’s Horizon 2020 research and innovation programme and Germany, Netherlands, Austria, Romania, France, Sweden, Cyprus, Greece, Lithuania, Portugal, Italy, Finland, Turkey.

Kontakt:

Christian Reil, M.Eng.

Ostbayerische Technische
Hochschule (OTH) Amberg-Weiden
Fakultät Elektrotechnik, Medien
und Informatik
Kaiser-Wilhelm-Ring 23
92224 Amberg

ch.reil@oth-aw.de

Patrick Purucker, M.Sc.

Ostbayerische Technische
Hochschule (OTH) Amberg-Weiden
Fakultät Elektrotechnik, Medien
und Informatik
Kaiser-Wilhelm-Ring 23
92224 Amberg

p.purucker@oth-aw.de

Nicholas Jäger, M.Sc.

Ostbayerische Technische
Hochschule (OTH) Amberg-Weiden
Fakultät Elektrotechnik, Medien
und Informatik
Kaiser-Wilhelm-Ring 23
92224 Amberg

n.jaeger@oth-aw.de

Prof. Dr.-Ing. Alfred Höß

Ostbayerische Technische
Hochschule (OTH) Amberg-Weiden
Fakultät Elektrotechnik, Medien
und Informatik
Kaiser-Wilhelm-Ring 23
92224 Amberg

a.hoess@oth-aw.de

Prof. Dr. Andreas Aßmuth

Ostbayerische Technische
Hochschule (OTH) Amberg-Weiden
Fakultät Elektrotechnik, Medien
und Informatik
Kaiser-Wilhelm-Ring 23
92224 Amberg

a.assmuth@oth-aw.de