Forschungsprojekt: ADACORSA "Airborne data collection on resilient system architectures"

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

Zusammenfassung

Drohnen verfügen im zivilen Bereich über ein großes Potenzial, welches aber gegenwärtig dadurch limitiert wird, dass Drohnen noch nicht zuverlässig (teil-) autonom außerhalb der Sichtweite operieren können und dies auch nicht dürfen. Das Ziel des von der EU und den nationalen Behörden geförderten Forschungsprojekts ADACORSA (https://www.adacorsa.eu/) besteht primär darin, die technischen Komponenten für Drohnen zu entwickeln, die Flüge außerhalb der Sichtweite ermöglichen. Die Ostbayerische Technische Hochschule Amberg-Weiden trägt dazu im Bereich zuverlässige und sichere Kommunikation bei: Sie entwickelt Modelle zur Vorhersage von Quality of Service Parametern für die Drohnenkommunikation über das Mobilfunknetz (zuverlässige Kommunikation). Ferner entwickelt sie Systeme zur Authentifizierung und zum Trust-Management in Flying Ad-hoc Networks (sichere Kommunikation).

Abstract

Drones have a great potential in the civilian section, but this potential is currently limited by the fact that drones cannot yet operate reliably (semi-) autonomously beyond visual line of sight and furthermore it is not allowed. The primary goal of the research project ADACORSA (https://www.adacorsa.eu/), which is funded by the EU and national authorities, is to develop the technical components for drones that enable flights beyond visual line of sight. The Technical University of Applied Sciences Amberg-Weiden contributes to this project in the field of reliable and secure communication: It develops quality of service prediction models for drone communication based on cellular networks (reliable communication). It also enables systems for authentication and trust management in flying ad-hoc networks (secure communication).

1 Einleitung

Seit einigen Jahren erfreuen sich Drohnen bzw. unbemannte Luftfahrzeuge (UAVs - Unmanned/Uncrewed Aerial Vehicles) im zivilen Bereich zunehmender Beliebtheit (militärische Drohnen bzw. militärische Anwendungen werden nicht betrachtet). Gegenwärtig werden sie hauptsächlich als fliegende Kameras eingesetzt, um beispielsweise beeindruckende Luftaufnahmen zu machen, oder um große Anlagen, wie Windräder und Fotovoltaikanlagen, auf Schäden zu überprüfen. Neben ihrer Funktion als fliegende Kameras finden Drohnen auch im Sport- und Freizeitbereich Verwendung, z. B. in Drohnenrennen oder als Spielzeug. Darüber hinaus besitzen UAVs eine große Anzahl an vielversprechenden Einsatzmöglichkeiten im zivilen Bereich, wie z. B.: Frachtdrohnen können durch Verwendung der dritten Dimension die Verkehrsnetze entlasten oder an Ziele liefern, die nur schwer oder unwirtschaftlich zu erreichen sind (z. B. Inseln). Ein weiteres Einsatzfeld von Drohnen besteht in der Überwachung von Gelände oder von Objekten. Sie könnten beispielsweise Wälder auf Waldbrände überwachen oder auf Wildtierbestände. In der Form von Such- und Rettungsmissionen können sie große oder schwer zugängliche Gebiete nach (bestimmten) Menschen absuchen, die Hilfe benötigen, beispielsweise nach Lawinen in Bergen. Im Bereich Katastrophenhilfe könnten sie zum Löschen von Bränden eingesetzt werden oder zum Aufbau einer Notfallinfrastruktur [1].

Um das volle Potenzial der Drohnentechnologie ausschöpfen zu können, bedarf es technischen Weiterentwicklungen und entsprechend angepassten rechtlichen

Rahmenbedingungen, damit die Drohnen im bestehenden Luftraum neben den bisherigen Luftverkehr fliegen können und dürfen. Eine Schlüsselfähigkeit dafür besteht darin, dass Drohnen BVLOS (Beyond Visual Line of Sight, außerhalb der Sichtverbindung) operieren können (siehe Abbildung 1). Dafür benötigen Drohnen ein hohes Maß an Autonomie, Zuverlässigkeit, Sicherheit sowie Kommunikations- und Kooperationsfähigkeit. Die dazu erforderliche zuverlässige Hard- und Software ist gegenwärtig im kommerziellen Bereich für Drohnen nicht verfügbar und muss noch entwickelt werden. Durch die Forschung und Entwicklung im Bereich von vernetzten und autonomen Fahrzeugen wurden Hardware- und Software-Komponenten entwickelt, die für den Einsatz in Drohnen voraussichtlich adaptiert werden können.

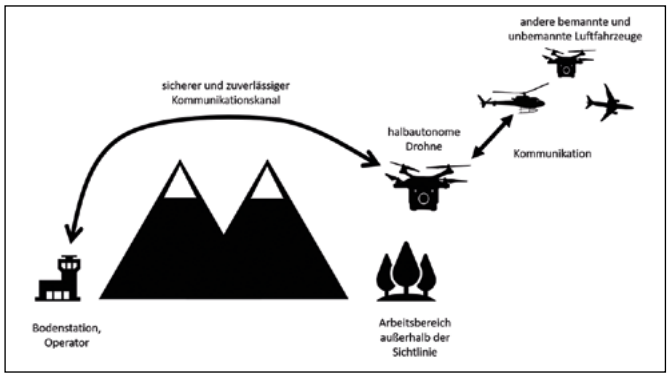

Abbildung 1: schematische Darstellung des BVLOS-Szenarios

Das Hauptziel des von der EU und nationalen Behörden geförderten Forschungsprojekts **“Airborne data collection on resilient system architectures” (ADACORSA)** besteht darin, die technischen Komponenten (Hardware, Software) bereitzustellen, die es teilautonomen UAVs ermöglichen, BVLOS-Flüge im kontrollierten und unkontrollierten Luftraum durchzuführen [2]. Dabei werden sowohl neue technische Komponenten entwickelt als auch Komponenten aus der Automobilbranche verwendet.

Die im ADACORSA geplanten Aktivitäten lassen sich fünf Hauptgebieten zuordnen: Luftfahrtelektronik für Drohnen, Kommunikationstechnologie und Infrastruktur, rechtliche Rahmenbedingungen, Sicherheit und gesellschaftliche Akzeptanz.

Im ADACORSA-Projekt arbeiten 49 europäische Partner aus zwölf Staaten (Deutschland, Finnland, Frankreich, Griechenland, Italien, Litauen, Niederlande, Österreich, Portugal, Schweden, Türkei und Zypern) zusammen und bringen die Erfahrungen aus unterschiedlichen Branchen ein (Luftfahrt, Automobilbranche, Halbleiterindustrie, Forschung und Bildung). Das Projekt startete im Mai 2020 und hat eine geplante Laufzeit von drei Jahren.

Die Projektaktivitäten sind thematisch in zehn Supply Chains organisiert, die jeweils ein übergeordnetes Ziel verfolgen. Die Aktivitäten der Ostbayerischen Technischen Hochschule Amberg-Weiden (OTH AW) finden primär in Supply Chain 4 “Security and reliability of communication and identification of drones and operators” statt. Die Aufgabe dieser Supply Chain besteht darin, die technologischen Komponenten (Hardware, Software usw.) zu entwickeln, um eine sichere, schnelle und zuverlässige Kommunikation zwischen BVLOS-fähigen Drohnen untereinander und mit der Bodenstation zu ermöglichen. Die OTH AW liefert dabei Beiträge sowohl im Bereich der zuverlässigen als auch im Bereich der sicheren Kommunikation, die in den Abschnitten 2. Zuverlässigkeit von mobilfunkbasierter Kommunikation von Drohnen und 3. Vertrauensbasierte Sicherheit in Flying Ad-hoc Networks (FANETs) vorgestellt werden.

2 Zuverlässigkeit von mobilfunkbasierter Kommunikation von Drohnen

Für BVLOS-Flüge von Drohnen ist ein zuverlässiger Kommunikationskanal essenziell, damit der Operator der Drohne das Verhalten der Drohne überwachen und gegebenenfalls eingreifen kann. Für die Kommunikation stehen verschiedene Technologien zur Verfügung, wie z. B. Mobilfunk, Bluetooth, Satellitenverbindungen oder WLAN, welche unterschiedliche Verbindungscharakteristiken aufweisen (Reichweite, Latenz, Datendurchsatz) und für unterschiedliche Situationen geeignet sind. Je nach Situation können die Daten auch über mehrere Kommunikationskanäle unter Verwendung verschiedener Technologien parallel übertragen werden. Das Ziel der OTH AW besteht darin, Modelle zu entwickeln, um die Verbindungsqualität (QoS – Quality of Service) des Mobilfunks vorherzusagen und diese in verschiedenen Algorithmen zu verwenden. Beispielsweise kann die Trajektorie der Drohne entsprechend der prädizierten QoS-Werte angepasst werden. Diese Vorgehensweise ist in Abbildung 2 visualisiert.

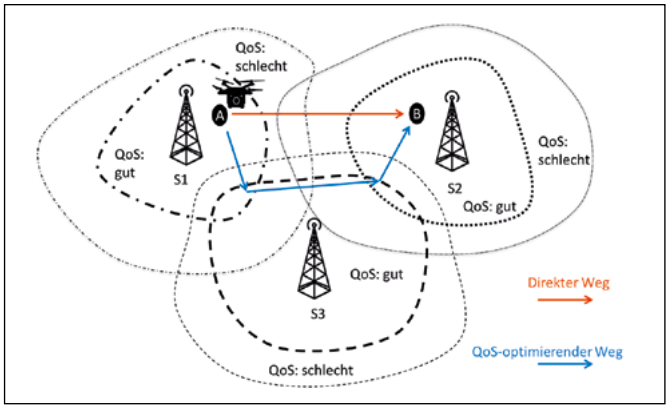

Abbildung 2: schematische Darstellung eines QoS-basierten Routings.

Die geplante Arbeit lässt sich in sechs Phasen einteilen: Analyse, Messung, Modellierung, Prädiktion, Integration. Um die Ergebnisse nach der Integration anhand des Demonstrators zu bewerten, werden im Rahmen von

ADACORSA zunächst die Anforderungen an das Kommunikationsgateway und der Stand der Technik hinsichtlich der Mobilfunkkommunikation betrachtet. Nach 3GPP [3] können die zu übertragenden Daten in Applikationsdaten und Steuerungsdaten, auch Command and Control Data (C&C), aufgeteilt werden.

Unter Applikationsdaten versteht man beispielsweise Sensordaten oder auch Bild-/Videodaten. Diese Daten sind im Vergleich zu C&C-Daten zeitunkritisch, wobei Latenzen in einem Bereich kleiner 400 ms angestrebt werden [4]. Allerdings werden für hochauflösende Videodaten Bandbreiten im Uplink von bis zu 50 Mbps benötigt [3]. C&C-Daten werden dagegen zum Steuern des UAV verwendet. Die Steuerung kann dabei direkt oder auch in Form von Wegpunkten erfolgen, wobei für die direkte Steuerung deutlich höhere Anforderungen an Latenz und Datenrate erforderlich sind und eine Videoübertragung nötig ist [5]. Für die direkte Steuerung liegt die nötige Latenz bei 40 ms und die Datenrate bei 60-100 kbps [5], [3]. Die Zuverlässigkeit des Kommunikationskanals sollte bei C&C-Daten mindestens 99,9 % betragen [5].

Um die geforderten Übertragungscharakteristiken im BVLOS-Bereich umzusetzen, wird im Rahmen des Forschungsprojektes die Datenübertragung mithilfe der aktuellen Long Term Evolution (LTE) Technologie und des künftigen 5th Generation (5G) Netzwerk genauer betrachtet.

3 Vertrauensbasierte Sicherheit in FANETs

Aufgrund ihres großen Potenzials stellen Drohnen ein attraktives Angriffsziel für Hacker dar (vgl. beispielsweise [6]). Die Angriffsfläche der Drohne erhöht sich, wenn diese (teil-) autonom operieren oder in offenen Umgebungen kommunizieren, indem sie FANETs bilden. Es ist daher unverzichtbar, die Kommunikation der Drohnen mit entsprechenden Sicherheitsmaßnahmen abzusichern, um Angriffe abzuwehren, abzumildern und zu protokollieren.

FANETs sind Ad-hoc-Netzwerkstrukturen, die von den UAVs aufgespannt werden, um miteinander zu kommunizieren (vgl. [7]). Man kann sie als eine Art Vehicular Ad-hoc Network (VANET) bzw. Mobile Ad-hoc Network (MANET) auffassen. Sie unterscheiden sich jedoch in einigen Aspekten, wie z. B. Dichte, Mobilitätsverhalten und Leistungsfähigkeit der Netzwerkknoten voneinander. Daher können Sicherheitskonzepte von VANETs bzw. MANETs übernommen werden, die jedoch aufgrund der Unterschiede an die Situationen in FANETs angepasst werden müssen, da sie ansonsten weniger wirkungsvoll sind, versagen oder sogar neue Sicherheitsprobleme erzeugen.

Der Beitrag der OTH AW zur sicheren Kommunikation besteht in der Entwicklung eines Authentifikationssystems und eines Trust-Management-Systems für FANETs, welche vertrauensbasierte Sicherheitsmaßnahmen darstellen. Vertrauensbasierte Sicherheit basiert auf Mechanismen, die zwischenmenschlichem Vertrauen (mehr oder weniger) ähneln. Die Vertrauenswürdigkeit anderer Kommunikationsteilnehmer wird mithilfe eigener Informationen (direktes Vertrauen) und Fremdinformationen (indirektes bzw. vermitteltes) Vertrauen eingeschätzt und für die weitere Interaktion berücksichtigt.

Die Hauptaufgabe des Authentifikationssystems besteht darin, die Identität des Kommunikationspartners zu verifizieren. Dadurch wird es möglich, sichere Kommunikationskanäle aufzubauen. In offenen Netzen werden bevorzugt Public-Key-Infrastrukturen (PKI) benutzt, welche die Verwendung von Public-Key-Kryptografie ermöglichen, indem Identitäten mit öffentlichen Schlüsseln (public keys) mittels Zertifikate verknüpft werden. Die Verknüpfung der Schlüssel basiert dabei auf Vertrauensbeziehungen und einem Vertrauensmodell, welches regelt, wann ein Schlüssel als vertrauenswürdig eingestuft werden kann. Weit verbreitet sind hierarchische PKIs, die auf zentrale Vertrauens- und Informationsinstanzen (Zertifizierungsstellen) setzen. Nur die Zertifizierungsstellen verfügen über das Recht, Zertifikate anderen Teilnehmern, einschließlich anderer Zertifizierungsstellen, auszustellen und zurückzurufen, wodurch eine Zertifikatshierarchie entsteht. Dieses System ist in den Zertifizierungsstellen zentralisiert, die attraktive Angriffsziele darstellen. Im Kontext autonomer Systeme, die auch ohne zentrale Instanz funktionsfähig sein sollten, können dezentrale PKIs Alternativen darstellen. In dezentralen Systemen darf prinzipiell jeder Teilnehmer anderen Teilnehmern Zertifikate ausstellen und die selbst ausgestellten Zertifikate widerrufen. Dabei müssen die Teilnehmer bei jedem anderen Teilnehmer entscheiden, ob sie diesem vertrauen. Das Vertrauensmodell und bestehenden Vertrauensbeziehungen ermöglichen es, die Vertrauenswürdigkeit anderer Teilnehmer einzuschätzen, sofern es gemeinsame Bekannte gibt. Das Ziel der OTH AW besteht darin ein dezentrales Authentifikationssystem für (teil-) autonome UAVs zu entwickeln.

Während ein Authentifizierungssystem die Identitäten verifiziert und somit regelt, wer am Netzwerk partizipieren kann, ist es die Aufgabe des Trust-Management-Systems, das Verhalten der verschiedenen Teilnehmer zu bewerten. Ohne ein Trust-Management-System könnte ein authentifizierter Teilnehmer sich bösartig verhalten (und damit Schäden anrichten), ohne zeitnahe Sanktionen befürchten zu müssen. Das Trust-Management-System identifiziert und isoliert Teilnehmer, die sich nicht regelkonform verhalten. In MANETs und VANETs sind Trust-Management-Systeme bereits gut erforscht, während die Forschung im Bereich FANETs erst am Anfang steht (vgl. beispielsweise [8]). Die OTH AW wird ein leistungsfähiges Trust-Management-System für FANETs entwickeln.

Die Entwicklung eines Trust-Management-Systems lässt sich in verschiedene Schritte gliedern: Zunächst müssen die Szenarien und damit das Bewegungs- und Kommunikationsverhalten festgelegt werden, für die das System ausgelegt werden soll. Darauf aufbauend wird ein Grundmodell entwickelt, wofür verschiedene Methoden zur Verfügung stehen, wie z. B. Expertensysteme, Maschinelles Lernen (neuronale Netze, evolutionäre Algorithmen) und statistische Verfahren. Um die Parameter des Modells zu bestimmen, sind umfangreiche Computersimulationen notwendig, die das Verhalten der UAVs und der Angreifer in den festgelegten Szenarien abbilden, da nicht hinreichend viele Daten aus der echten Welt vorliegen. Nachdem durch die Simulationen aussichtsreiche Parameterkonstellationen gefunden wurden, müssen diese durch weitere Simulationen, die verschiedene Elemente, wie z. B. das Verhalten und Anzahl der UAVs und Angreifer variieren, ergänzt werden, um die Leistungsfähigkeit zu bestimmen.

4 Zusammenfassung

Das von der EU und nationalen Behörden geförderte Forschungsprojekt ADACORSA verfolgt das Ziel, die technischen Komponenten (Hardware, Software) zu entwickeln, um BVLOS-Flüge von (teil-) autonomen Drohnen zu ermöglichen. Dadurch erschließen sich im zivilen Bereich zahlreiche Anwendungsfälle, wie beispielsweise im Bereich der Logistik, wodurch die Verkehrsnetze entlastet werden können. Für BVLOS-fähige Drohnen ist eine sichere und zuverlässige Kommunikation erforderlich, damit die Drohne mit dem Kontrollzentrum Sensor- und Kommandodaten austauschen kann. Die OTH AW trägt im Bereich der zuverlässigen und sicheren Kommunikation zu dem Projekt bei, indem sie Modelle zur Vorhersage von QoS von Mobilfunkverbindungen sowie vertrauensbasierte Sicherheitssysteme (Authentifizierung, Trust Management) für FANETs entwickelt.

Referenzen:

[1] M. Christen, M. Guillaume, M. Jablonowski und K. Moll, Zivile Drohnen – Herausforderungen und Perspektiven, Zürich: vdf, 2018.

[2] „ADACORSA Website“, [Online]. Available: https://adacorsa.eu/.

[3] 3GPP, “TR 36.777 V15.0.0 Technical Specification Group Radio Access Network; Study on Enhanced LTE Support for Aerial Vehicles”, 12 2017. [Online]. Available: ftp://www.3gpp.org/specs/archive/36_series/36.777.

[4] G. Yang, X. Lin, Y. Li, H. Cui, M. Xu, D. Wu, H. Rydén und S. B. Redhwan, “A Telecom Perspective on the Internet of Drones: From LTE-Advanced to 5G”, *arXiv*, p. 8, 29 3 2018.

[5] 3GPP, “TS 22.125 V17.1.0 Technical Specification Group Services and System Aspects; Unmanned Aerial System (UAS) support in 3GPP”, 12 2019. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3545.

[6] K. Hartmann und K. Giles, “UAV exploitation: A new domain for cyber power”, in *2016 8th International Conference on Cyber Conflict (CyCon)*, Talinn, 2016.

[7] İ. Bekmezci, E. Şentürk und T. Türker, “SECURITY ISSUES IN FLYING AD-HOC NETWORKS (FANETs)”, *Journal of Aeronautics and Space Technologies*, Bd. 9, p. 13 – 21, 25 7 2016.

[8] K. Singh, K. A. Verma und P. Aggarwal, “Analysis of Various Trust Computation Methods: A step toward Secure FANETs”, in *Computer and Cyber Security – Principles, Algorithm, Applications, and Perspectives*, CRC Press, 2018, pp. 171 – 193.

Projektpartner:

Acknowledgement:

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.

Das Bundesministerium für Bildung und Forschung (BMBF) fördert das Projekt unter dem deutschen Titel „Verbundprojekt: Sichere Elektronik- und Sensorsysteme für autonome Luftfahrzeuge – ADACORSA" mit dem Teilvorhaben an der OTH Amberg-Weiden „Sichere, zuverlässige und vertrauenswürdige Kommunikation für Drohnen" unter der Fördernummer 16MEE0039.

ECSEL JU

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Kontakt:

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

Patrick Purucker, B.Eng.

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

p.purucker@oth-aw.de

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

Prof. Dr.-Ing. Alfred Höß

Ostbayerische Technische
Hochschule (OTH) Amberg-Weiden
Fakultät Elektrotechnik,
Medien und Informatik
Vizepräsident Forschung und
Technologietransfer,
wissenschaftlicher Nachwuchs
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
Wissenschaftlicher Leiter
des Rechenzentrums
Kaiser-Wilhelm-Ring 23
92224 Amberg

a.assmuth@oth-aw.de