ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Ondřej Vítovec

HROZBY PŮSOBÍCÍ NA BEZPILOTNÍ SYSTÉMY A OBRANY PROTI NIM

Bakalářská práce

2019

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
děkan
Konviktská 20, 110 00 Praha 1

K621 ..... **Ústav letecké dopravy**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Ondřej Vítovec

Kód studijního programu a studijní obor studenta:

B 3710 – TUL – Technologie údržby letadel

Název tématu (česky): **Hrozby působící na bezpilotní systémy a obrany proti nim**

Název tématu (anglicky): Threats to Unmanned Aerial Systems and Their Protection

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte osnovou uvedenou v následujících bodech:

- Obecný popis bezpilotních systémů
- Analýza existujících způsobů obrany proti hrozbám působících na bezpilotní systémy
- Vyhodnocení způsobů obran proti hrozbám působících na bezpilotní systémy
- Návrh změn a vylepšení současných obranných systému bezpilotních systémů
- Vlastní návrh konfigurace vybavení na obranu určitého bezpilotního systému

Rozsah grafických prací: dle pokynů vedoucího bakalářské práce

Rozsah průvodní zprávy: minimálně 35 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury:
SADIKU, Matthew N.O. Principles of Electromagnetics. 4th Edition. 2009

CHAMAYOU, Grégoire. A Theory of the Drone. 2015.

KLIMEŠ, Bohdan a Josef Bartoloměj SLAVÍK. Elektromagnetické vlny. 1958

Vedoucí bakalářské práce: **Ing. David Hůlek**

Datum zadání bakalářské práce: **19. října 2018**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání bakalářské práce: **26. srpna 2019**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE Fakulta dopravní L.S.

doc. Ing. Jakub Kraus, Ph.D.
vedoucí
Ústavu letecké dopravy

doc. Ing. Pavel Hrubeš, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání bakalářské práce.

Ondřej Vítovec
jméno a podpis studenta

V Praze dne ..... 19. října 2018

Poděkování

Tímto bych rád poděkoval všem, kteří mě při mém studiu podporovali. Velký dík pak patří zejména Ing. Davidu Hůlkovi, Ph.D. za odborné vedení mé bakalářské práce a za poskytnuté konzultace, které pro mne byly vždy velice přínosné. V neposlední řadě také děkuji celé své rodině, zvláště pak rodičům, za všechnu podporu, které se mi od nich během celého dosavadního studia dostalo.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Nemám závažný důvod proti užívání tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 12.08.2019 ……

……
podpis

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

HROZBY PŮSOBÍCÍ NA BEZPILOTNÍ SYSTÉMY A OBRANY PROTI NIM

Bakalářská práce
srpen 2019

Ondřej Vítovec

Abstrakt

Cílem této bakalářské práce nazvané „Hrozby působící na bezpilotní systémy a obrany proti nim“ je poskytnout srozumitelný, ucelený přehled těchto hrozeb a situací, za kterých k nim dochází, a také podrobně popsat nebo navrhnout různé možnosti obran bezpilotních systémů (UAS) proti těmto hrozbám. V úvodu práce je zařazena kapitola popisující bezpilotní systém jako celek a jeho hlavní části. Stěžejní část práce poté tvoří popis jednotlivých hrozeb působících na bezpilotní systémy v jeho běžném provozu a také popis možných obran proti popisovaným hrozbám. Příkladem časté vážné hrozby je kolize UAS ve vzduchu s jiným objektem nebo také útok na jeho komunikační a navigační systémy. Veškeré hrozby a jejich obrany pro lepší přehlednost shrnují dvě vytvořené tabulky. V poslední části bakalářské práce je vytvořen návrh pro vybavení ústavního UAS Phantom 3 Standard od společnosti DJI.

Klíčová slova

bezpilotní systém, bezpilotní letadlo, řídící stanice, UAS, hrozby, obrany, protisrážkový systém, DSA, komunikační prostředky, útok, sestřelení

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Transportation Sciences

THREATS TO UNMANNED AERIAL SYSTEMS AND THEIR PROTECTION

Bachelor's Thesis
August 2019
Ondřej Vítovec

Abstract

The main aim of this bachelor thesis, entitled "Threats to Unmanned Aerial Systems and Their Protection", is to provide a comprehensive overview of threats to unmanned aerial systems (UAS) and situations in which they arise, as well as to offer a solutions and ways in which UAS may prevent such threats. The introductory part includes a chapter describing UAS as a whole and their major components. The main body of the thesis comprises a description of a number of threats UAS may face during operation and the protection against them. An example of commonly encountered significant threat is a collision of the UAS with another flying object or an attack on the UAS communication and navigation systems. All threats and protections against them are summarised in two comprehensive tables. The final part of the thesis includes a proposed design of the equipment of the Department's DJI Phantom 3 Standard UAS.

Key words

unmanned aerial system, unmanned aircraft, control station, UAS, threats, protection, collision avoidance system, DSA, means of communication, attack, shooting down

Obsah

Seznam použitých zkratek

ABSAA	Airborne Sense and Avoid	
ACAS	Airborne Collision Avoidance System	Palubní protisrážkový systém
ADS-B	Automatic Dependent Surveillance – Broadcast	Automatický závislý přehledový systém
AFCS	Automatic Flight Control System	Automatický systém řízení
BAMS-D	Broad Area Maritime Surveillance Demonstrator	
CRPA	Controlled Radiation Pattern Antennas	Anténa schopna mapovat prostorovou různorodost signálů
DAIDALUS	Detect and Avoid Alerting Logic for Unmanned Systems	
DGPS	Differential Global Positioning System	Diferenciální globální systém určení polohy
DoS	Denial of Services	Odmítnutí služeb
DSA	Detect, Sense and Avoid	
EMP	Electromagnetic Pulse	Elektromagnetický puls
FAA	Federal Aviation Administration	Federální letecký úřad
FTP	File Transfer Protocol	Služba pro přenos souborů na internetu
GBSAA	Ground-Based Sense and Avoid	

GLONASS	Global Orbiting Navigation Satellite System, rusky: ЛОбальная НАвигационная Спутниковая Система, tr.: Globalnaja navigacionnaja sputnikovaja sistěma	Globální navigační systém na oběžné dráze
GNSS	Global Navigation Satellite System	Globální navigační satelitní systém
GPS	Global Positioning System	Globální systém určení polohy
ICAO	International Civil Aviation Organization	Mezinárodní organizace pro civilní letectví
ICMP	Internet Control Message Protocol	Protokol používající síťová zařízení pro zasílání chybových zpráv a provozních informací
LOAM	Laser Obstacle Avoidance and Monitoring	Protisrážkový systém využívající technologii laseru
4G LTE	Fourth Generation Long-Term Evolution	Technologie určená pro vysokorychlostní internet v mobilních sítích
MAC	Media Access Control	MAC adresa je jednoznačný identifikátor síťového zařízení
MitM	Man in the Middle	Označení bezdrátového útoku, kdy je potřeba připojit se mezi vysílač a přijímač
MOPS	Minimum Operational Performance Standards	Standardy minimální provozní výkonnosti
NASA	National Aeronautics and Space Administration	Národní úřad pro letectví a kosmonautiku

NextGen	Next Generation Air Transportation System	Systém nové generace pro bezpečný provoz v oblasti letového provozu
RA	Resolution Advisory	Rada k vyhnutí
RAM	Radar Absorbent Materials	Materiály pohlcující radarové vlny
RCS	Radar Cross Section	Odrazová plocha radarového záření
RFID	Radio Frequency Identifier	Radiofrekvenční identifikace
SAR	Synthetic Aperture Radar	Radar se syntetickou aperturou
SD	Secure Digital	Zkratka používaná ve spojení s SD kartou
SIM	Subscriber Identification Module	Identifikační karta účastníka
SSID	Service Set Identifier	Identifikátor bezdrátové sítě
TA	Traffic Advisory	Upozornění na blížící se provoz u protisrážkových systémů
TCAS	Traffic Alert and Collision Avoidance System	Provozní výstražný protisrážkový systém
TRM	Threat Resolution Module	Modul, používaný v systému ACAS-Xu, pro kontrolu úhybného manévru
UA	Unmanned Aircraft	Bezpilotní letadlo
UAS	Unmanned Aerial System	Bezpilotní systém
UHD	Ultra High Definition	Ultra vysoké rozlišení
U.S.	United States	Spojené státy

USA	United States of America	Spojené státy americké
UV	Ultraviolet	Ultrafialové záření
ÚLD	Department of Air Transport	Ústav letecké dopravy

Úvod

Bezpilotní letadla jsou dnes velmi často skloňovaným pojmem, a to nejen v mediích. Přitom ještě nedávno byla myšlenka bezpilotních systémů jako celku spíše pojmem teoretickým. Dnes se již s těmito systémy můžeme setkat téměř na každém rohu. Navzdory tomu, že jedno z prvních bezpilotních letadel bylo testováno již v polovině 19. století, do povědomí veřejnosti se bezpilotní systémy začaly dostávat až z počátku století jednadvacátého. Pravdou je, že ono zmíněné první bezpilotní letadlo byl balón, který s dnešní vyspělou technikou neměl společného prakticky nic. Naopak v průběhu 20. století, s příchodem možnosti ovládat letadlo vzdáleně skrze rádiové vlny, se tento nový typ letadel začal ve vzduchu objevovat poměrně často. Z historie také víme, že bitvy většinou vyhrál ten, kdo měl o celém bojišti lepší přehled. Již od nepaměti se tedy vojevůdci snažili vymyslet stále dokonalejší možnosti mapování oblastí, kde se skrýval nepřítel nebo kde se měla odehrát samotná bitva. Ten samý cíl měli pravděpodobně konstruktéři prvních pozorovacích balónů nebo vzducholodí. S příchodem letounů bylo nově možno sledovat nepřátelské pozice daleko za hranicemi vlastního území. Nicméně letouny s posádkou na palubě při svých misích často riskovaly životy právě své posádky. [15] Toto, ale i další potřeby lidstva, přispělo k vývoji bezpilotních systémů, které dnes slouží nejen k čistě vojenským potřebám, ale i ke komerčnímu využití, například ve filmařském průmyslu nebo také jako volnočasová aktivita dostupná téměř každému. Právě díky této rozšířenosti bezpilotních systémů v komerčním sektoru se v práci nebudu věnovat jen čistě vojenským nebo naopak jen nevojenským aplikacím bezpilotních systémů.

Faktem je, že bezpilotní systémy jsou takřka v permanentním nebezpečí. A to ať už se jedná o vojenské, či civilní bezpilotní systémy. U prvních zmiňovaných jsou tyto hrozby ještě znásobeny z povahy jejich činnosti. Tomu také odpovídá i stupeň jejich obranného vybavení. Na druhou stranu i u vojenských bezpilotních systémů se můžeme setkat s absencí určitých obranných systémů, protože se do jejich strojů prostě nevejde kompletně veškeré dostupné vybavení. U civilních bezpilotních systémů se v dnešní době můžeme setkat se základním protisrážkovým systémem, který výrazně ochraňuje stroj před srážkou s terénem a v určitých situacích dokonce i před srážkou s jiným letícím objektem.

Celkový souhrn různých ochran proti hrozbám není v žádné dostupné literatuře k dispozici. Většina literatury na toto téma je výhradně v anglickém jazyce a téměř vždy se věnuje jen jednomu úzkému okruhu ohrožení bezpilotního stroje případně obraně

proti takovému ohrožení. Příkladem takové literatury je kniha „Sense and Avoid in UAS: Research and Application“. Autorem této knihy je Plamen Angelov, který pojednává o problematice začlenění spolehlivého systému „*Sense and Avoid*” (blíže popsáno v následujících kapitolách) do bezpilotních systémů. Touto prací je vytvořen souhrn základních hrozeb, se kterými se mohou setkat jak vojenské, tak i civilní bezpilotní systémy. Ke každé hrozbě, případně celé skupině, je pospána nebo navrhnuta vhodná obrana, díky které by byl bezpilotní systém v běžném provozu proti této hrozbě efektivně ochráněn.

Na samém začátku práce je však nutné obecně popsat čtenáři bezpilotní systém jako celek, princip jeho funkce a poté také jeho základní části, bez kterých nelze bezpilotní systém provozovat. Poměrně velká část práce je věnována obranám proti srážce bezpilotního letadla s terénem, kterou vnímám jako všudypřítomnou hrozbu v případě civilních bezpilotních systému. V případě vojenských bezpilotních systémů je tato hrozba přítomna minimálně v době vzletu a přistání bezpilotního letadla. V relativně blízké budoucnosti se pak počítá s výrazným navýšením počtu aktivně létajících bezpilotních systémů různých kategorií, a tudíž budou muset být ochráněny především před srážkou s jiným letícím letadlem nebo bezpilotním systémem ve vzduchu. [30]

Další část práce je věnována bezdrátovému narušení komunikace mezi řídící stanicí bezpilotního systému a jeho letadlem, což vzhledem k době, ve které žijeme, opět vnímám jako velmi aktuální hrozbu pro především civilní bezpilotní systémy. Následuje přehled dalších hrozeb, které mohou bezpilotní systém přímo fyzicky ohrozit. Tím je myšleno především sestřelení nebo například lapení bezpilotního letadla do sítě. Do této kapitoly jsem zařadil i poněkud netradiční ohrožení bezpilotního systému a tím je jeho napadení dravým ptákem. Pro tuto hrozbu jsou popsány dva druhy plašení ptáků. Jde o zvukové a vizuální plašičky, které by ve vhodné kombinaci měly přispět k úspěšnému zastrašení dravce.

V závěru jsem poté vytvořil dvě tabulky, které přehledně shrnují veškeré hrozby a obrany proti nim zmíněné v této bakalářské práci. První tabulka, věnující se protisrážkovým systémům, navíc ukazuje jednotlivé výhody a nevýhody veškerých popisovaných protisrážkových systémů. Jako poslední kapitola této bakalářské práce je vlastní návrh obranného vybavení pro stroj DJI Phantom 3 Standard. Ten je k dispozici na Ústavu letecké dopravy (ÚLD), na Fakultě dopravní pro jeho zaměstnance i studenty. Obranné vybavení tohoto stroje je navrhnuto pro budoucí činnosti bezpilotního systému na Ústavu.

1 Obecný popis bezpilotních systémů

UAS *(Anglicky: Unmanned Aerial System)* jsou různé bezpilotní systémy, které je vždy nutno brát jako celek. Takový systém je složen z několika subsystémů, kterými jsou například bezpilotní letadlo (*Anglicky: Unmanned Aircraft – UA)*, jeho náklad, řídící stanice, popřípadě subsystém pro vypuštění a přistání letadla nebo další subsystémy pro komunikaci. V dnešní době nesmíme opomínat fakt, že bezpilotní systémy jsou součástí leteckého průmyslu, který má jasně daná pravidla ve formě zákonů, předpisů, norem nebo nařízení. Jak je známo, sofistikované bezpilotní systémy dnes využívají armády po celém světě, nicméně jak již bylo řečeno, tato práce nebude zaměřena striktně na vojenské využití UAS, ale také na civilní. Tyto komerční bezpilotní letadla s vlastním ovládáním, které si může zakoupit každý z nás, jsou již svým vybavením na tak vysoké úrovni, že mají schopnost létat poměrně daleko od své řídící stanice, to znamená mimo dohled pilota, což je v České republice momentálně zakázáno. [16] Zejména tedy uživatelé, kteří mají doma tento jednoduchý UAS, si často všechna pravidla neuvědomují a létají na místech, kde je provozování bezpilotních systémů legislativně omezeno nebo dokonce zakázáno. Tímto svým nedbalým jednáním pak mohou způsobit nemalé komplikace například v letecké dopravě, kdy mohou vyřadit z provozu celá letiště na několik hodin.

Bezpilotní systémy se od těch, které mají pilota na palubě, liší především tím, že musí umožnit bezpečné ovládání a přenášení důležitých parametrů do řídící stanice a naopak. To klade nemalé nároky na bezpečnost komunikace nebo kvalitu přenášeného signálu mezi UA a řídící stanicí. Díky absenci posádky na palubě může být toto místo využito například pro uložení palubních počítačů nebo pro uskladnění nákladu. Běžně ale UAS nejsou určeny pro přepravu rozměrných nákladů, takže díky absenci člověka na palubě mohou být bezpilotní letouny menší a kompaktnější. To se projevuje i na pokroku techniky, kdy dokážeme do stále menších prostor vměstnat stále více systémů, které jsou oproti starším ekvivalentům o mnoho výkonnější. Většinu dalších subsystémů, kterými jsou UAS vybaveny, najdeme i na systémech, které na palubě řídí člověk. [17]

V médiích se velmi často objevují zavádějící označení pro bezpilotní systémy, které jsou sice pro lajky lépe zapamatovatelné, ale rozhodně se nejedná o správné pojmenování bezpilotních systémů. Musíme mít na paměti, že žádné hovorové označení bezpilotních systémů není uvedeno v platných předpisech, nařízeních či odborné literatuře. V médiích se však bohužel tato nesprávná označení bezpilotních systémů objevují, což dále napomáhá k šíření nekorektního názvosloví pro UAS napříč veřejností. Dále si

nesmíme plést pojmy UAS/UA s pojmem „model letadla“, u kterého je uživatel úzce limitován jen na základní řízení modulu, bez výrazného technického vybavení. [18]

Moderní bezpilotní systémy mají povětšinou větší nebo menší stupeň umělé inteligence. Součástí jsou bezpilotní letouny, které jsou schopny řídící stanici předávat živý obraz z například termokamer společně s datovým balíkem, který obsahuje nezbytná data o poloze, rychlosti, kurzu a výšce. Mimo to samozřejmě dokážou pozemní řídící stanici předávat i sekundární data, jakými jsou například teploty oleje, výkon motorů, množství paliva a další. V případě, že se nějaký ze subsystémů porouchá, může být UAS naprogramován tak, že přinejmenším informuje svého pilota o problému, popřípadě sám vykoná příslušné úkony pro vyřešení nastalé krizové situace. Kupříkladu, pokud selže komunikace mezi UA a jeho řídící stanicí, může být celý UAS naprogramován tak, aby sám začal prohledávat dostupné radiové frekvence a na některé z nich se sám pokusil obnovit spojení mezi stanicí a letadlem. Další, ještě více pokročilou funkcí, může být schopnost naprogramovat UAS příkazy „jestliže“ se stane toto, „pak“ proveď danou akci. Některé moderní bezpilotní systémy jsou vybavovány vyššími stupni umělé inteligence, které do jisté míry umožňují úplnou samostatnost systému v případě řešení některých situací. Neměli bychom opomenout, že za bezpilotní systémy se nepovažují řízené střely, naváděné rakety, které se při útoku zničí, ani jiné jim podobné zbraně. [1]

Odborných definic pro bezpilotní systémy je několik, nicméně vždy se jedná o velmi podobnou definici, která se obsahově neodlišuje od ostatních. Za závaznou definici bychom mohli pokládat tu, kterou vydal Úřad pro civilní letectví České republiky. Podle něj je bezpilotní systém (UAS) takový systém, který se *„skládá z bezpilotního letadla, řídicí stanice a jakéhokoliv dalšího prvku nezbytného k umožnění letu, jako například komunikačního spojení a zařízení pro vypuštění a návrat. Bezpilotních letadel, řídicích stanic nebo zařízení pro vypuštění a návrat může být v rámci bezpilotního systému více.“* [16]

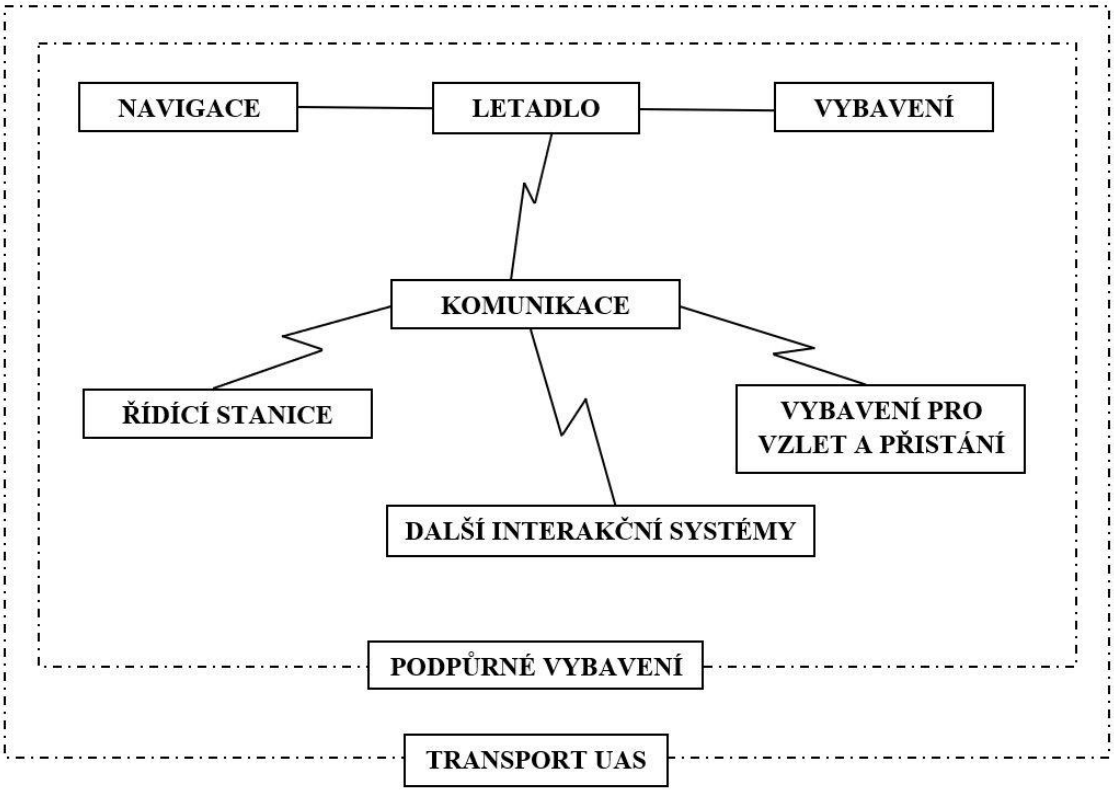
Bezpilotní letadlo je v Doplňku X předpisu L 2 definováno jako letadlo, které je *„určené k provozu bez pilota na palubě.“*, kdy pro účely Doplňku X se *„bezpilotním letadlem rozumí všechna bezpilotní letadla kromě modelů letadel s maximální vzletovou hmotností nepřesahující 25 kg.“* [18]

1.1 Princip funkce bezpilotních systémů

Technicky vzato se bezpilotní systém skládá z více prvků neboli subsystémů. Bezpilotní letoun je bezpečně tím nejvýraznějším, musíme však pamatovat na to, že UAS jako celek by se neobešel bez žádného ze subsystémů, které obsahuje. Technicky funkční struktura typického bezpilotního systému je zobrazena na Obrázku 1. Samozřejmě

existují i další aspekty, úzce spojené s fungováním bezpilotního systému, které na uvedeném obrázku nenajdeme. Je jím například povolení k letu v dané oblasti, pokud jde o lety v řízené oblasti nebo pokud je toto povolení k letu zapotřebí z jiného důvodu.

Jestliže nahlížíme na některý subsystém UAS, tak je nutné, abychom ho vnímali jako integrovanou součást systému, bez kterého by byla celková funkčnost UAS více či méně omezena. Jak již bylo řečeno, pro UAS jsou si všechny subsystémy rovnocenné, ačkoli subsystém, kterým je i bezpilotní letoun, jistě bude mít větší dopad na finální design bezpilotního systému než kupříkladu jeho navigační systém. [12]



Obrázek 1 - Struktura typického UAS, [1]

1.2 Hlavní části bezpilotního systému

V následující části bakalářské práce jsou stručně popsány stěžejní podsystémy, které mimo jiné najdeme na Obrázku 1. Tyto subsystémy jsou absolutně nezbytné pro běžné fungování bezpilotního systému. Bezpilotní systém samozřejmě obsahuje mnohem více podsystémů, než je uvedeno na Obrázku 1 nebo než popisuje tato práce. Tudíž je nutné říct, že tato kapitola má čtenáři pouze přiblížit základní princip a části bezpilotních systémů, takže zde není prostor pro veškeré systémy nebo části UAS, které se dnes běžně na bezpilotní systémy instalují.

1.2.1 Řídící stanice

Pod pojmem řídící stanice bezpilotního systému si lze představit poměrně širokou škálu možných aplikací. V této kapitole jsou roztříděny alespoň ty základní druhy řídících stanic, se kterými se v dnešní době po celém světě operuje. Řídící stanice se dají rozdělit na dvě základní skupiny.

První jsou takzvané přenosné řídící stanice, které mohou být ve formě dálkového ovládání. Tyto dálkové ovladače jsou dnes používány především u bezpilotních systémů pro komerční nebo domácí použití. Navíc je u některých z nich jejich důležitou součástí uživatelův chytrý telefon, bezdrátově propojený s dálkovým ovládačem, sloužící jako malý informační panel, na kterém mohou být zobrazeny různé informace o letounu nebo na něj může být přenášen živý obraz. Jejich ekvivalentem může být kombinace notebooku, joysticku a vysílače/přijímače, jako je tomu například u dnes již starší přenosné stanice Rotomotion SR20 GCS. Tato přenosná zařízení mají velkou výhodu v jejich kompaktnosti a možnosti využití prakticky kdekoliv po světě. Celkově jsou však velmi limitovány na kapacitu akumulátorů energie a výkonnost vysílačů a přijímačů. [19]

Druhou skupinou jsou pozemní stanice, které jsou umístěny buď na zemi, pak jde o čistě pozemní řídící stanice, nebo na palubě lodi či letadla. Kontrolní stanice slouží k interakci člověka a bezpilotního systému. Po většinou jsou tyto řídící stanice využívány nejen k přímému ovládání letadla, ale také k přípravě letového plánu, určení souřadnic různých traťových nebo cílových bodů apod. Tuto možnost plánování mají k dispozici i uživatelé rekreačních bezpilotních systémů, kde k vytvoření trasy letu používají převážně svůj chytrý telefon s kompatibilní aplikací. Ve vojenských případech mohou samozřejmě cíle anebo traťové body vytvořit v řídícím středisku na druhém konci světa a do řídící stanice daného bezpilotního systému je předat pouze k jejich vykonání. Z kontrolní stanice je tedy prostřednictvím up-linku zprostředkovaná jednosměrná komunikace mezi člověkem a bezpilotním letadlem. Díky tomu jsme schopni dávat letounu příkazy ke změně letu nebo k ovládání jeho vybavení. Letadlo „odpovídá“ díky down-linku, který řídící stanici dává schopnost přijímat informace z ovládaného letadla. Tyto informace jsou zejména balíčky telemetrických dat, obraz nebo informace z různých podsystémů UA. Kontrolní stanice je také stěžejním systémem pro komunikaci s externími systémy. Těmi mohou být například systémy poskytující data o počasí nebo jiná síť, poskytující dané informace velícímu středisku a podobně. [4]

1.2.2 Bezpilotní letadlo

Druhým podsystémem bezpilotních systémů je bezpilotní letadlo samotné. V současnosti existuje několik typů bezpilotních letadel, které se mezi sebou častokrát podstatně liší. Determinujícím faktorem pro typ UA je bezpochybně jeho budoucí pole působnosti. To zahrnuje jak operační prostředí, tak i vybavení, které si při své práci UA ponese na palubě. I proto dnešní trh zahrnuje nepřeberné množství druhů bezpilotních letadel, které poměrně celistvě pokrývají veškeré pole poptávky. Můžeme uvést příklad, kdy se hodí, aby se UA pohybovalo jen velmi pomalu nebo aby bylo schopné vertikálního stoupání a klesání. Uzpůsobení jeho motorů bude těmto podmínkám vyhovovat a tvar bezpilotního letadla bude také dozajista jiný než tvar UA, které bude určené pro cestovní rychlosti vyšší než kupříkladu 500 km/h s konvenčním startem a přistáním. Vybavení bezpilotního letadla zahrnuje několik dalších subsystémů. Mezi ty základní patří především jeho navigační a komunikační systémy, systém pro ovládání letu, motory a zdroj paliva nebo elektrické energie. V neposlední řadě nesmíme zapomenout na nezbytné vybavení pro plnění úkolů daného UAS. Příkladem tohoto vybavení může být prostá kamera, ale také síť pro přepravu zavěšeného nákladu. [3]

Pro představu je uvedeno jedno z mnoha možných dělení bezpilotních letadel, a to dělení dle funkčních kategorií [6]:

- Průzkumné
- Bojové
- Logistické
- Civilní a komerční
- Výzkumné a vývojové
- Cíle a návnady

Z názvů výše popsaných kategorií je zřejmé pole působnosti daného bezpilotního letadla. Dalším možným způsobem třídění bezpilotních letadel může být kupříkladu řazení v závislosti na hmotnosti nebo dle uspořádání a typu pohonných jednotek. [6] Nicméně veškeré možné způsoby třídění bezpilotních systémů nelze v této práci obsáhnout, jelikož je dané téma již za hranicemi jejího obsahu.

1.2.3 Navigace

Pro dnešní provoz bezpilotních systémů je absolutně nezbytné, aby byly vybaveny zařízením, díky kterému je určena pozice letadla řízeného z řídící stanice. Dnes je hojně využíván GPS (*Anglicky: Global Positioning System*), poskytující informace o pozici díky satelitům kroužících okolo Země. GPS se stal velmi dostupným i pro nevojenské účely a jeho implementace do UAS je dnes již banální záležitostí. Před systémem GPS museli

stroje využívat inerční navigační systémy, kde jejich instalace na palubu letadla byla náročná nejen díky jejich velikosti, ale také velké hmotnosti. Přesnost systému GPS může být ještě větší, pokud se využije systém DGPS, kde „D“ na začátku zkratky značí anglicky *Differential* neboli diferenciální. Tento systém tak nevyužívá pouze satelity GPS, ale i speciální pozemní stanice, díky kterým se zpřesňuje odchylka v takzvaných pseudovzdálenostech, a tím je i přesnější výsledná určená pozice DGPS přijímače. Pro neautonomní operace, kdy je třeba, aby řídící stanice měla přehled o pozici kontrolovaného letadla, je nutné mít ještě záložní systém pro určení jeho pozice v případě, že by byl GPS signál blokován nebo nějakým způsobem rušen. Uvedeny jsou pouze tři základní možnosti [20]:

1) První možností je „dopočítávání“ aktuální pozice letadla pomocí vektorů rychlosti a uplynulého času z poslední správně určené pozice. Jde o jednu z nejzákladnějších metod určování pozice. V angličtině je tento druh navigace nazýván jako *Dead* nebo *Direct reckoning*. Do češtiny by se tento způsob mohl přeložit jako stanovení polohy přibližným výpočtem.
2) Druhou základní metodou určování pozice letadla bez systému GPS a systémům jim podobným, je takzvaný *Radio tracking.* Systém využívá rádiový signál, který přenáší data z letadla do řídící stanice. Azimut, tedy směr k letadlu, určí řídící stanice podle toho, z jakého směru signál přijala. Vzdálenost pak dopočítává díky času, za jaký signál urazí danou vzdálenost od letadla k řídící stanici.
3) Třetí možností je vybavit letadlo odpovídačem sekundárního radaru, který odpovídá na dotazy odeslané řídící stanicí. Tyto odpovědi obsahují základní informace o pozici, rychlosti nebo také směru letu letadla. V tomto případě jde o takzvaný *Radar tracking*. [21]

K určení alespoň přibližné pozice při výpadku systému GPS by se dal také použít primární radar, který funguje na principu odrazu vln od letícího tělesa. Nicméně pro bezpilotní systémy se tento způsob nejeví jako úplně vhodný. Jednak jsou letadla bezpilotních systémů relativně malá, tudíž by vlny z primárního radaru nemusely být dostatečně odraženy a tím by letoun nebyl primárním radarem detekován. Větší bezpilotní systémy využívané především armádami jsou zase mnohdy konstruovány tak, aby se od nich vlny z primárních radarů odrážely minimálně nebo vůbec, tudíž k detekci primárním radarem také nedojde. Pro zlepšení viditelnosti UAS primárním radarem je také možné instalovat na UA speciální odrazové plochy, díky kterým lze i relativně malé UA sledovat pomocí primárního radaru. Dle mého názoru, tedy není možné použít primární radar jako plnohodnotný systém k určení pozice, který by v krizové situaci mohl nahradit například systém GPS.

1.2.4 Komunikace

Mezi stěžejní subsystémy bezpilotních systémů dozajista patří systém komunikační. Bez něho by letadlo bez posádky na palubě nebylo schopno plnit žádné úkoly, které mu díky up-linku přichází z pozemní řídící stanice. Mezi informace, které up-linkem putují z řídící stanice do UA, patří například přenos letového plánu, který je následně v UA uložen v automatickém systému řízení (*Anglicky: Automatic Flight Control System – AFCS*) [22]. Dále je díky up-linku možné vzdáleně UA řídit nebo také předávat povely pro další subsystémy UA. Pomocí down-linku naopak bezpilotní letadlo předává informace řídící stanici. Zde jde především o vysílání balíčků dat polohy UA, přenášení dat a/nebo médií, které shromažďují další subsystémy UA a také zde probíhá přenos základních dat z bezpilotního letadla. Řídící stanice tak pomocí down-linku dostává celkový obraz o stavu a chování bezpilotního letadla a také o tom, co se děje v jeho okolí. [1]

Pro většinu komerčních bezpilotních systémů, při letech na větší vzdálenosti od řídící stanice, odpadá možnost přenášet například obraz živě do zařízení, které je na zemi. Je to z důvodu, že pro živý přenos médií využívají komerční bezpilotní systémy především sítě Wi-Fi, které pracují na vysokofrekvenčních kmitočtech 2.4 GHz nebo až 5.8 GHz, a pro které je maximální vzdálenost přenosu podstatně menší. To je způsobeno tím, že tyto krátké vlny nejsou schopny dobře prostupovat překážkami, a tudíž se jejich signál velmi snadno utlumí. Frekvence 2.4 GHz je dnes také nejpoužívanější frekvencí pro domácí Wi-Fi připojení, což opět v obydlených oblastech způsobovalo rušení signálu mezi UA a jeho řídící stanicí. Pokud UAS tedy používal pouze jednu frekvenci, jak pro ovládání letadla, tak pro přenos medií, často zde docházelo k vzájemnému rušení. V některých případech se tedy přešlo k modelu, kdy UAS využívá pásmo frekvenci 5.8 GHz k přenosu signálu pro ovládání UA z řídící stanice a frekvence 2.4 GHz se využívá pro přenášení dat a médií z UA do kontrolní stanice [23].

Pro přenos dat na větší vzdálenosti se nabízí využití rádiové vlny o nižších frekvencích. Řádově jde o frekvence okolo 900 MHz. Tyto frekvence pracující s delšími vlnami, snadněji procházejí skrze překážky, ovšem potřebují k vyslání, respektive přijetí signálu větší anténu, což může být problém především u menších UAS [24]. Vhodným řešením pro komerční bezpilotní systémy se zdá být využití mobilního internetu. Nejmodernější modelové řady komerčních bezpilotních systémů již nabízí integrovaný 4G/LTE modem, skrze který lze hladce přenášet živý obraz kamkoli po internetu. [25] Pro využití si ovšem uživatel musí pořídit kartu SIM, podporující rychlé 4G mobilní připojení a s UA musí operovat pouze v dosahu signálu mobilních sítí. Komerční bezpilotní systémy také často využívají k aktualizaci softwaru nebo k uchování medií a jiných dat integrované sloty pro SD karty, skrze které lze daná data snadno uchovávat a pracovat s nimi. Vojenské

bezpilotní systémy využívají ke komunikaci především bezpečné satelitní připojení v kombinaci s data linkem, který spojuje UA a jeho řídící stanici [26]. Typická mise vojenského UAS nazývaného Predator probíhá tak, že vzlet a přistání UA jsou řízeny přímo z řídící stanice, která musí být v přímém rádiovém spojení s UA. Nezbytné je to proto, že při řízení UA pomocí satelitního spojení, dochází ke zpoždění signálu až o dvě sekundy, což právě při kritických situacích, jakými jsou vzlet a přistání, může způsobit poškození nebo dokonce zničení UA. Samotný let a zbytek mise je pak řízen skrze satelitní připojení například z vojenské základny v umístěné na klidně na druhé straně světa. Skrze satelity je pak pro oprávněné zařízení možné po celou dobu mise sledovat údaje a data z UA. [27]

Celková úroveň složitosti celého komunikačního systému UAS se odvíjí od celkové spotřeby elektrické energie, komplexnosti zpracování a vyhodnocení dat, konstrukčního řešení samotné antény, hmotnosti a ceny. Proto je nutné vždy vytvořit komunikační systém, který bude konstruovaný na míru dle budoucího využití UAS. Výše zmíněné faktory, které výrazně ovlivní výslednou podobu komunikačního systému jsou odvozeny z následujících požadavků. Vzdálenost, na jakou je UA schopno komunikace s pozemní řídící stanicí, sofistikovanost dat z UA a jeho subsystémů, které je nutno bezdrátově předat do řídící stanice a v neposlední řadě také úroveň zabezpečení přenosu. Tyto požadavky se vzájemně liší při různých využitích UAS a je tedy nutné systém komunikace nakonfigurovat tak, aby splnil daný účel, ale aby se zároveň dosáhlo optimální hmotnosti, díky které je pak UA agilnější a schopné setrvat ve vzduchu o něco déle.

2 Protisrážkové systémy pro UAS

Jedna z největších hrozeb, které je bezpilotní systém během svého užívání prakticky nepřetržitě vystaven, je bezpochyby srážka s terénem nebo s jiným letícím objektem. Pro bezpilotní systémy je naprosto nezbytné, aby disponovaly určitým typem systému ochraňující je před případnou srážkou. Oproti letadlům, která mají pilota na své palubě, jsou UAS v nevýhodě, protože jsou řízeny z řídící stanice, kde pilot nemá tak dokonalý vizuální přehled o prostoru kolem UA. Tato kapitola je tedy zaměřena na protisrážkové systémy, díky kterým se mnohonásobně zvyšuje ochrana UAS před zničením, které by bylo po srážce s terénem nebo s jiným letícím objektem takřka nevyhnutelné.

V posledních letech se využití bezpilotních systémů v civilním i necivilním sektoru razantně navyšuje a je tedy jasné, že v budoucnu budou UAS létat v mnohem větším množství po boku letadel s piloty na palubě. Toto tvrzení potvrzuje i Federální letecký úřad (*Anglicky: Federal Aviation Administration – FAA*) USA, který předpokládá, že se prodeje UAS pro „domácí“ použití mezi roky 2016 a 2020 v USA více než zdvojnásobí. V roce 2016 zde bylo prodáno 1,9 milionu UAS a předpoklad pro rok 2020 je až 4,3 milionu prodaných „domácích“ UAS. Dále tento dokument uvádí zvýšení prodeje komerčně zaměřených bezpilotních systémů z 600 000 kusů prodaných v roce 2016 až na 2,7 milionu kusů v roce 2020. [28] Tento strmý nárůst bezpilotních systémů používaných v USA dokládá i statistika počtu zaregistrovaných bezpilotních systémů úřadem FAA. V březnu roku 2017 bylo v USA registrováno celkem 770 000 komerčních i „domácích“ uživatelů UAS. V lednu roku 2018 celkový počet takových registrací pokořil hranici jednoho milionu. Tato statistika je však co do počtu UAS nepřesná, protože ve Spojených státech se majitel, který hodlá používat UAS nekomerčně, registruje pouze jednou, a přitom může vlastnit více UAS. FFA díky tomu předpokládá, že na začátku roku 2018 bylo v provozu již kolem 1,5 milionu UAS. [29]

Rozmach bezpilotních systémů se dále projevuje i ve vojenském sektoru. Podle studie, která vznikla ve spolupráci Ministerstva dopravy USA a Letectva Spojených států amerických, bude v roce 2035 pouze ve Spojených státech zhruba 14 000 kusů UAS v provozu pro Ministerstvo obrany USA a dalších zhruba 70 000 kusů bude potřeba pro státní organizace. Právě v roce 2035 mají podle této studie UAS překonat počet letadel s piloty na palubě ve vojenském a komerčním sektoru. [30]

Aby tedy bylo možné zařadit UAS do běžného provozu bok po boku letadel s posádkou na palubě, je nezbytné, aby tyto UAS byly vybaveny protisrážkovým systémem, který by v daných situacích upozornil na vzniklé riziko a případně by zcela autonomně katastrofě zabránil. Již v roce 2007 spustila NASA (*Anglicky: The National Aeronautics and Space Administration*), spolupracující s Letectvem spojených států, program pro vývoj systému, jehož hlavním cílem by bylo odvrátit případnou kolizi s cizím objektem. [31]

2.1 Počátek protisrážkových systémů UAS

Z výše popsaných skutečností je jasné, že UAS budou muset disponovat určitým protisrážkovým systémem. Jelikož v oblasti vývoje bezpilotních systémů byla vždy v čele armáda Spojených států, i vývoj prvních protisrážkových systému probíhal pod jejím zaštítěním. Jedním z prvních kroků k protisrážkovým systémům UAS bylo vytvoření počítačového modelu, s cílem určit správné programy k simulaci a také otestovat schopnosti radaru správně detekovat jak kooperující, tak nekooperující překážky. Mezi takzvané kooperující neboli spolupracující překážky na trase letu UAS bychom mohli zařadit civilní letadla vybavená odpovídajícím typem softwaru, zatímco mezi nekooperující překážky se řadí například budovy, parašutisté nebo privátní letouny. K simulaci bylo zvoleno využití radaru se syntetickou aperturou (*Anglicky: Synthetic Aperture Radar – SAR*) a tři bezpilotní systémy. Tyto tři UAS byly typu Predator RQ-1, Predator RQ-1A a Predator MQ-9B. Testovaný systém měl vyhovět předem daným požadavkům, kterými bylo například vyhodnocení situace jako „konfliktní“ při jakékoli vzdálenosti obou UAS menší než 500 stop. Dále vydat varování před srážkou v čase 45 sekund před bodem nejmenšího přiblížení obou UAS a v neposlední řadě vydat takzvanou Radu k vyhnutí (*Anglicky: Resolution Advisory – RA*) v čase 30 sekund před bodem nejmenšího přiblížení UAS. Je nutné dodat, že při této simulaci nebyly využity systémy ani data z TCAS (Traffic Collision Avoidance System), ADS-B (Automatic Dependent Surveillance – Broadcast), ani funkce autopilota. Tento počítačový model se ukázal jako velmi vhodný k budoucímu vývoji protisrážkových systémů pro UAS, neboť prokázal schopnost UAS se autonomně vyhnout kolizi s druhým UAS a následně se vrátit zpět do svého kurzu a pokračovat dál v letu. Tato studie počítá s pokračujícím vývojem protisrážkových systémů UAS, kde by byly zapojeny senzory z TCAS a ADS-B, aby došlo ke zvýšení bezpečnosti letů UAS. Pro další vývoj se počítá se spoluprací agentury NASA s Letectvem a Námořnictvem Spojených států amerických, což ukazuje, že vývoj protisrážkového systému UAS byl a stále je prioritním projektem Americké vlády. Tato studie dále poukazuje na to, že vybavit bezpilotní systém plně autonomním protisrážkovým systémem bude vyžadovat výrazné zásahy do vybavení i do konstrukce UAS. [31]

2.2 Detect, Sense and Avoid (DSA)

Detect, Sense and Avoid, zkráceně DSA ve volném překladu znamená detekovat, vycítit a vyhnout. Detekcí *(detect)* je myšleno zjištění, za pomoci různých druhů technologií, že se ve sledovaném prostoru vyskytuje překážka. Zde je nutné dodat, že detekce je odlišná od identifikace, a tedy nedochází k rozlišení druhu nebo typu překážky. Vycítit *(sense)* znamená rozhodnout, zdali je detekovaný objekt pro UAS hrozbou, či nikoli. Tento proces tedy započne ihned po detekování potenciální překážky a díky sérii algoritmů proběhnou výpočty, které vedou k rozhodnutí o tom, jeli objekt hrozbou nebo není. Tyto algoritmy se dají přirovnat k mozkové činnosti, která probíhá v situaci, kdy se pilot v kokpitu svého letadla dostane do situace, kdy musí rozhodnout mezi setrváním na daném kurzu nebo započetím úhybného manévru pro vyhnutí se překážce. Vyhnutí *(avoid)* je pak proces samotného úhybného manévru, vyhnutí se překážce a následné vrácení se zpět do původního kurzu. Pro UAS je naprosto nezbytné disponovat právě těmito vlastnostmi, které jsou v DSA ukryty a díky kterým jsou schopny předat informace, popřípadě sami vyřešit krizovou situaci a umožnit bezpečné vyhnutí se případné srážce s překážkou. Vytvoření DSA vedla prakticky od samotného začátku FAA, která v minulosti po dlouhou dobu využívala jako primární metodu pro odvrácení nehody především piloty na palubě letadla a jejich rozhled. FAA tedy musela vymyslet způsob, jakým zrak pilota z kokpitu v UAS nahradí. S postupným začleňováním stále více UAS pro civilní, komerční i vojenské účely do vzdušného prostoru, je nezbytné, aby disponovaly danými DSA systémy, díky kterým bude zaručen určitý stupeň bezpečnosti. [32, 33]

Cílem systémů DSA je tedy v kritických situacích hrozících srážkou pracovat stejně dobře nebo dokonce lépe, než kdyby byla na palubě přítomna posádka [34]. V roce 2004 vyšel Dokument F2411-04 (dnes je po úpravách označován jako F2411-04e1), který se zabývá standardy specifikací pro design a výkonnost vzdušného systému Sense-and-Avoid. Anglicky je tento dokument také nazýván „*Standard Specification for Design and Performance of an Airborne Sense-and-Avoid System*.“ Tento dokument je klíčový, protože od jeho vydání slouží jako zásady pro developery a výzkumné pracovníky bezpilotních systémů. Rámcově tento dokument obsahuje dvě složky pro požadavky na UAS. První částí dokument specifikuje požadavky na detekci a bezpečnou separaci UAS od okolního provozu. Druhá část poté vytyčuje obecný výhled z letadla s posádkou na palubě. Tato druhá část dokumentu tedy stanovuje, že UAS musí být svým vybavením schopné detekovat překážky při ustáleném horizontálním letu, nacházející se v jeho zorném poli o výseči ±110° azimutálních a úhlové výšce ±15° [32]. V pozdějších studiích se pracuje s vyššími hodnotami, protože pro pokročilé

protisrážkové systémy je ideální, aby měly přehled v rozsahu 360° okolo sebe. Tyto hodnoty tedy nahrazují a vylepšují zorné pole pilota, který v UA chybí [31]. Dokument dále po DSA vyžaduje reakci na odvrácení kolize v dostatečném čase, pokud se v popsaném zorném poli UAS objeví narušitel. Nejbližší bod přiblížení obou letadel musí být větší než 500 stop, které jsou obecně definovány jako vzdálenost, kdy téměř dojde ke kolizi letadel ve vzduchu. [32]

Vybavení bezpilotních systémů systémy pro DSA je nezbytné, aby byl zachován co nejvyšší stupeň bezpečnosti. Abychom splnili například přísné certifikační procesy FAA nazývané jako *„Technical Standard Order“* musí systémy DSA plnit pět základních funkcí, přičemž na každou funkci jsou kladeny různé požadavky [32]:

i) *Detekce provozu v konfliktním kurzu* – požadavek pro první funkci DSA je především spolehlivé kontinuální snímání výše zmíněné výseče o daných úhlech ±110° azimutálních a ±15° úhlové výšky, dále „sledovat“ všechny hrozby v daném minimálním dosahu. Zároveň však minimalizovat počet falešných detekcí hrozeb a minimalizovat počet hrozeb, které DSA vůbec nedetekuje. Poslední požadavek je stanovit rychlost přibližování k překážce a poskytovat operátorovi UAS data o dané hrozbě.

ii) *Určení Right of Way (přednosti)* – její požadavky jsou takové, aby buď autonomně nebo za pomoci operátora UAS učinil UAS takovou změnu dráhy letu, která odpovídá nařízením FAA/ICAO (*Anglicky: International Civil Aviation Organization*).

iii) *Analyzovat dráhu letu* – Stanovit, zdali se potenciální hrozba pohybuje směrem ke konfliktní zóně a vypočítat možné letové dráhy na základě poskytnutých dat ze senzorů a aktualizovat čas potřebný k manévru.

iv) *Manévr* – Manévr musí být proveden podle postupů FAA. Operátor UAS může zasáhnout do řízení během daného manévru. Manévr musí být dokončen i v případě ztráty signálu s řídící stanicí UAS. V průběhu manévru musí být zachován daný minimální rozestup 500 stop. Po dokončení vyhýbacího manévru se UAS musí vrátit do původního kurzu.

v) *Komunikace* – Systém musí spojitě předávat informace řídící stanici. Operátorovi UAS musí být umožněno převzetí řízení. Dále musí být dostupná vlnová pásma pro přenesení datových balíčků. Prioritní komunikace musí sloužit k zachování bezpečnosti letu a systém musí podávat hlášení, pokud je objekt vyhodnocen jako nebezpečný a zároveň podávat možnosti pro úspěšné vyřešení problému až do doby, kdy je krizová situace úspěšně vyřešena.

V následující části bakalářské práce je ve zkratce popsáno několik základních technologií, které lze pro DSA systémy potencionálně využít. Tyto DSA technologie můžeme podle jejich funkce rozdělit do dvou velkých skupin. Jsou jimi technologie pro DSA takzvaně nekooperativní neboli nespolupracující a systémy kooperativní.

2.3 Nekooperativní DSA technologie

Hned na začátku této podkapitoly je nutné uvést, že nekooperativní systémy a technologie mají nepřekonatelnou výhodu v tom, že překážka, která se jim naskytne do cesty, nemusí být vybavena žádným speciálním systémem nebo odpovídačem, aby došlo k její detekci. Tyto nekooperativní systémy dokážou detekovat překážku, která se nachází jak na zemi, tak ve vzduchu. Dále lze tuto skupinu systémů dělit na nekooperativní systémy, které jsou buď aktivní nebo pasivní. Aktivní nekooperativní systémy vysílají různé elektromagnetické vlny, díky kterým jsou schopny detekovat překážku. Příkladem může být radar, laser případně sonar. Sonar však není pro použití ve vzduchu příliš vhodný, neboť ke své činnosti využívá čistě zvukové vlny. Ty se ve vzduchu šíří podstatně pomaleji než v hustějších médiích. Rychlost šíření zvukových vln je také zásadně ovlivněna teplotou prostředí, ve kterém se šíří. Ta se v atmosféře také podstatně mění s výškou letu. Sonar je tedy vhodný pro použití pod vodou, nikoli pro použití na létajících prostředcích jakéhokoli druhu. Pasivní nekooperující systémy fungují na principu detekce vln, které daná překážka sama vyzařuje. Mezi tyto systémy můžeme zařadit systémy pro detekci pohybu, elektro-optické detektory nebo také detektory infračerveného záření. [12]

2.3.1 Radar

Radar je typickým aktivním nekooperativním DSA systémem. Takzvaný primární radar vysílá elektromagnetické vlny a detekuje jejich odrazy od cíle/cílů. To má vedle výše zmíněných výhod nekooperativních technologií i své nevýhody. Tou hlavní je, že elektromagnetické vlny se ve vzdušném prostoru odrazí i například od velkého mračna, což způsobí jejich detekci. Dalšími nevýhodami může být vysoký potřebný výkon radaru, ale také nutnost elektronicky filtrovat nejrůznější šumy, které se k radaru odrazy dostanou.

V současnosti je pro UAS používán SAR, především díky své malé velikosti. Je nutné dodat, že SAR se hodí více na pozorování pozemních objektů. SAR je schopný vytvořit lepší obraz než klasický radar, nicméně pro správnou funkci SAR je nutné, aby byl UA s tímto radarem na palubě v pohybu. SAR totiž využívá pohyb své antény vůči pozorovaným objektům, díky čemuž nepotřebuje mít tak velkou anténu pro vytvoření úzkého a efektivního paprsku. [35]

Postupně dochází k dalšímu vývoji v radarových technologiích, především v případě SAR je testován 3-D SAR, který disponuje více anténami a je tak schopen vytvořit trojrozměrný obraz cíle. Nové generace radarů SAR jsou schopny zachytit a upozornit na pohyb, který pozemní cíle vykonaly. Radary jsou hojně využívány především pro svoji schopnost fungovat i v případech, kdy je pro tmu, mlhu nebo vysokou oblačnost nemožné použití jiných technologií. Při využití radaru je také nutné počítat s prodlevou, kterou signál potřebuje na cestu k cíli a zpět. Toto prodlení odpadá například u využití elektro-optických systémů. [36]

Radarové systémy však nejsou využívány jen pro detekci pozemních objektů, jsou schopny detekovat i objekty pohybující se ve vzduchu, nicméně tuto vlastnost nemají zdaleka všechny typy radarů. Dalo by se říct, že využít radar jako protisrážkový systém, který bude umět detekovat pouze cíle na zemi, se pro letící UAS nejeví jako příliš vhodný. Zde je dobré poznamenat, že detekce potenciálních pozemních překážek je nutná zejména při vzletu a přistání UA, kdy se většina vzdušných nehod odehraje v okruhu 3 mil od letiště a polovina z nich se navíc stane při výšce letu ne vyšší než 1000 stop. [37]

2.3.2 GBSAA

Příkladem poměrně nového systému využívající pro svou funkci pozemní radary, je systém nazvaný Ground-Based Sense and Avoid (GBSAA). Jde taktéž o aktivní nekooperativní DSA technologii. Tento systém byl vyvinut speciálně pro možnost volného pohybu bezpilotních systémů v blízkosti ostatního vzdušného provozu v řízených vzdušných prostorech tak, aby plně nahrazoval funkci pilota na palubě při detekci a vyhodnocování potencionálně nebezpečných situací pro UAS. [38] Systém GBSAA sbírá data z několika pozemních radarů a pomocí speciálního algoritmu vyhodnocuje situace ve vzduchu a předává je do své vlastní pozemní stanice, kde jsou tyto informace dále zobrazeny operátorovi systému GBSAA. GBSAA dokáže sbírat data až ze šesti radarů, které následně sloučí a vytvoří z nich skutečný obraz situace ve vzduchu a promítá ho na monitor operátorovi. Nicméně pro spolehlivý a samozřejmě přesný provoz tohoto systému jsou zapotřebí minimálně tři pozemní radary. [39]

GBSAA je vytvořený tak, aby dokázal pracovat i s již existující sítí pozemních radarů. K funkci není tedy nutné stavět další pozemní radary, pokud se v dané oblasti již tyto radary, splňující určité parametry, nacházejí. Pokud systém vyhodnotí situaci tak, že pravděpodobně dojde ke kolizi, upozorní operátora a zároveň vypočte optimální úhybný manévr. Operátor GBSAA se pak neprodleně spojí s pilotem bezpilotního systému, kterému tyto informace o manévru poskytne a dohlídne na jeho vykonání [39]. Systém

GBSAA je díky využití primárních radarů schopný detekovat všechny objekty, které se nacházejí v dosahu paprsků radarů, a tudíž nevyžaduje instalaci speciálního vybavení na palubu UA [40]. Nicméně, hned několik zdrojů uvádí, že systém GBSAA bude schopný také komunikace s palubním odpovídačem, pokud jím bude letadlo vybaveno. Tato kombinace u systému GBSAA, podobně jako je tomu u kombinace primárního a sekundárního radaru, zlepšuje celkovou schopnost systému správně detekovat letadlo, případně díky poskytnutým datům z odpovídače bude systém schopný lépe analyzovat celou krizovou situaci [41]. Zpočátku byl systém GBSAA vyvíjen čistě pro vojenské použití, takže nyní je v provozu na několika amerických vojenských základnách, nicméně tento systém je schopný se v budoucnu po určitých úpravách přizpůsobit i civilnímu využití. [38, 40]

2.3.3 Laser

Posledním nekooperativním aktivním systémem popsaným v této bakalářské práci, který lze využít pro DSA v bezpilotních systémech, je laser. Velký krok k využití laseru u DSA udělali ve společnosti SELEX Communications, kde vyvinuli Laser Obstacle Avoidance and Monitoring (LOAM®) [42]. Již na počátku 21. století začala společnost Lockheed Martin tento sytém testovat pro vojenská i civilní letadla s posádkou na palubě. Protisrážkové systémy, jakými je i LOAM, využívají pro oči člověka nezávadný laser, který v principu funguje velmi obdobně jako radar. Laser skenuje prostor před letadlem v pravidelných intervalech. Výsledky těchto „pozorování“ poté procházejí složitým softwarem, který analyzuje a vyhodnocuje možné překážky. Při testech ve společnosti Lockheed Martin zatím tento systém při detekci pouze vydal výstrahu pilotovi, který měl následně celému konfliktu zabránit. [2] Nicméně pro zcela autonomní využití v bezpilotních systémech je nezbytné, aby byl vyvinut software splňující požadavky například FAA, který by byl schopen zasáhnout správným způsobem do řízení bezpilotního systému a autonomně tak zabránil případné kolizi.

Velkou výhodou použití laseru je, že paprsky vyzářené laserem mají vysokou energii, a tak jsou schopny se odrazit nejen od velkých předmětů, jakými jsou například budovy, ale také od malých drátů do velikosti až pěti milimetrů v průměru. Stejně tak je systém laseru díky množství energie schopen detekovat i překážky, které nemají svůj povrch kolmý na vyzařovací paprsek laseru. Těmito objekty jsou velmi často například stromy nebo pouliční lampy. [2]

Laserové systémy je možné také v široké škále různě konfigurovat. Tato vlastnost se hodí například pro kompenzaci vlastností atmosféry, které se s rostoucí výškou letu razantně mění. I tato možnost konfigurace vede k tomu, že systém laseru je schopen eliminovat prakticky veškeré chybné odrazy paprsků laseru. [43] Eliminace chybných odrazů společně s vysokým rozlišením monitorované oblasti činí z laseru velmi efektivní a spolehlivý systém. Podle mého si laser, jakožto systém DSA, jistě najde uplatnění v budoucím použití v bezpilotních systémech.

2.3.4 Systém pro detekci pohybu

Systém pro detekci pohybu je prvním systémem spadajícím do pasivních nekooperativních DSA technologií. Tyto systémy, určené pro použití v letectví, se od běžně dostupných detektorů pohybu diametrálně liší. Zatímco detektory pohybu, které jsou využívány především pro zabezpečení objektů, dokážou pouze detekovat pohyb a v důsledku toho předat tuto informaci své řídící stanici. Pro případné využití v UAS je však nezbytně nutný mnohem sofistikovanější systém detekce pohybu. Byť se současné technologie takto pokročilých systémů pro detekci pohybu liší, většina z nich pracuje na obdobném principu. K detekci okolí je využíváno několik kamer, které jsou instalovány pod různými úhly, tak aby při spojení jejich obrazů mohl být softwarově dopočítán vektor pohybu pozorovaného objektu. [44] Jinými slovy můžeme říct, že obrazy z kamer jsou sjednoceny a software pak hledá různé odlišnosti v jednotlivých pixelech a z nich následně dopočítává vektor pohybu. Pro použití těchto systémů na bezpilotních letadlech je však nutno především software upravit tak, aby si uměl poradit s pohybujícím se okolím při samotném letu letadla. Tyto algoritmy zabývající se rozlišením pohybu vzniklým letem a pohybu cizího objektu se od sebe odlišují podle společností, které se výzkumem takového systému zabývají. Z pravidla má však tento algoritmus za úkol eliminovat pohyb samotného bezpilotního systému včetně vibrací, které jsou s jeho činností spojené.

Nabízí se zde také využití systému, který by napodoboval funkci oka létajícího hmyzu. Jak je známo, oči hmyzu jsou složeny z několika set malých oček zvaných omatidií. Oko složené z omatidií daleko lépe vnímá pohyb ve svém okolí, což se výborně hodí právě pro funkci systému pro detekci pohybu. [45] Vědci pro systém detekce pohybu „nahradili“ omatidii fotoreceptory, které spolu se softwarem dokážou zaznamenat pohyb objektu a následně určit jeho vektor pohybu.

2.4 Kooperativní DSA technologie

Mezi takzvaně spolupracující DSA systémy se řadí ty systémy, které využívají k detekci objektu jeho odpověď na vyslaný dotaz. Velmi známým příkladem takového kooperativního systému je sekundární radar. Ten také vysílá elektromagnetické vlny, ale již nedetekuje jejich odraz od objektu. Vlny jsou energeticky slabší a nesou v sobě pouze určitý „dotaz“. Pokud se tyto vlny dostanou k objektu, který je vybaven odpovídačem neboli transpodérem, na dotaz odpoví vysláním své vlastní odpovědí, která do sekundárního radaru dorazí a tím dojde k detekci objektu. Je zřejmé, že k detekci je nezbytně nutné, aby byl daný objekt takovým odpovídačem vybaven, jinak je pro takový systém detekce objektu nemožná. V praxi často dochází ke spojení obou, kooperativních i nekooperativních systémů, pro zlepšení přesnosti detekce takového systému. [12]

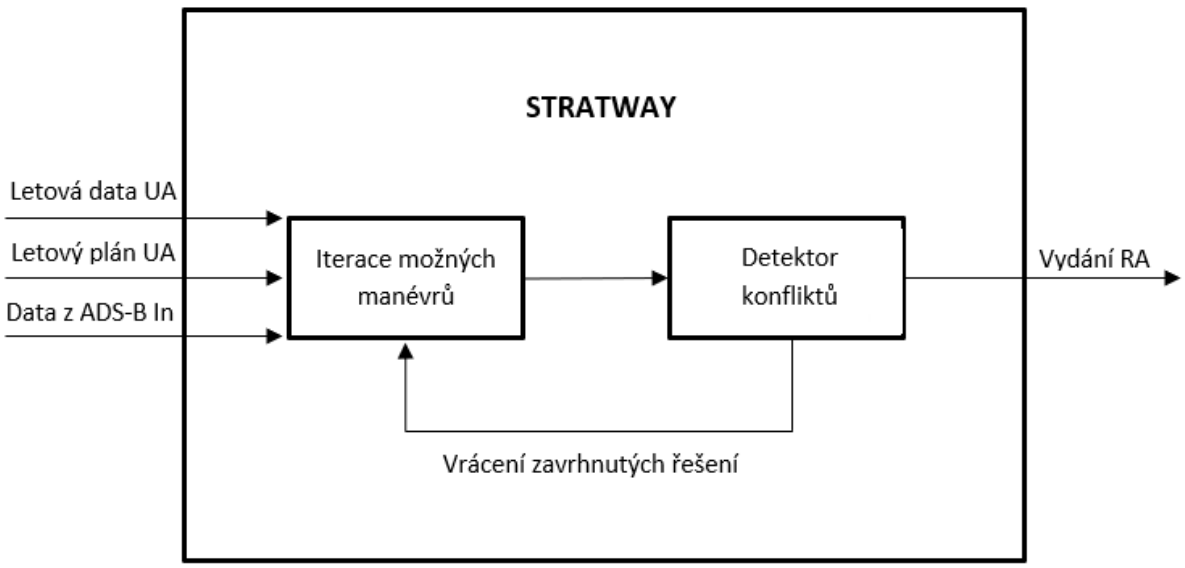
2.4.1 ADS-B jako DSA

Příkladem kooperativního systému DSA je přímé využití technologie ADS-B (*Anglicky: Automatic Dependent Surveillance – Broadcast*). Tato technologie přímo pomáhá zlepšit bezpečnost a celkovou efektivitu, kterou zajišťují řídící letového provozu. Celý systém ADS-B je složen ze dvou dílčích částí – *ADS-B In* a *ADS-B Out*, které mohou být instalovány zcela separovaně. První, tedy ADS-B In, slouží pouze k příjmu, zpracování a případnému poskytnutí ADS-B informací, které byly vyslány jiným letadlem. ADS-B Out poté zcela logicky plní funkci odeslání ADS-B informací z letounu do svého okolí. Je nutné podotknout, že ADS-B využívá k přenosu informací rádiové vlny. [46] ADS-B je systém závislý a zároveň kooperativní, což znamená, že k správnému přijetí ADS-B dat vyslaných letadlem vybaveným ADS-B Out, je nutné mít letadlo vybavené ADS-B In. Z toho vyplývá, že letadla nedisponující vybavením ADS-B In/Out, nejsou schopna přijmout ADS-B data a zároveň jsou pro ostatní letadla z pohledu ADS-B „neviditelná“. Díky schopnostem systému ADS-B FAA rozhodla, že od roku 2020 budou všechna letadla v NAS, třídě vzdušného prostoru A mít povinnost být vybavena právě systémem ADS-B. [47, 48]

2.4.2 Stratway

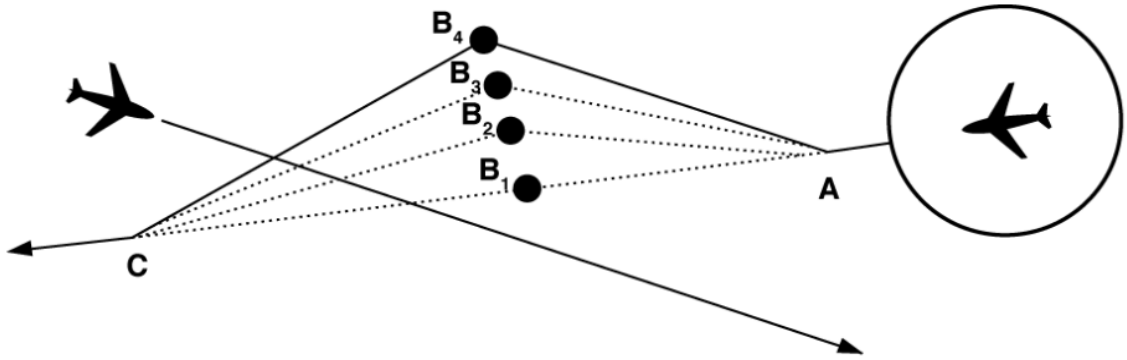
I díky výše zmíněné povinnosti se NASA rozhodla vytvořit algoritmus, který bude využívat data ADS-B a bude pro UAS poskytovat DSA, nezbytné k bezpečnému provozu v řízených vzdušných prostorech. Tento algoritmus by měl poskytnout pilotům bezpilotních systémů lepší přehled o situaci ve vzduchu. V případě, kdy by se jejich UA dostal na kolizní trajektorii s jiným letícím letadlem, algoritmus by vypočítal vhodný manévr, díky kterému by se UAS vyhnul hrozícímu nebezpečí. V NASA pracovali hned s několika algoritmy, přičemž po letech simulací a reálných testů byl jako nejvhodnější

kandidát vybrán algoritmus nazvaný Stratway. Tento algoritmus využívá modulární přístup pro výpočet nejvhodnějšího úhybného manévru. Podobně jako u dalších DSA systémů se musí tento algoritmus vhodně upravit pro každý typ UAS, aby při výpočtu vhodného manévru nedošlo k překročení letové obálky. Schéma, jak algoritmus pracuje vidíme na Obrázku 2. Zjednodušeně toto schéma můžeme pospat takto: Vstupní data pro algoritmus jsou letová data z letounu, jeho letový plán a ADS-B data přijímaná z letadla, které se nachází na kolizním kurzu. Na základě těchto vstupů algoritmus navrhuje možné úhybné manévry. Tyto manévry procházejí skrze „detektor konfliktu“, který pečlivě zkoumá, zdali je daný manévr po celou dobu skutečně bezpečný, tudíž zdali se jeho provedením dostane UA mimo konfliktní kurz a vyhne se tak možné srážce a následně se bez dalšího hrozícího nebezpečí vrátí do původního kurzu. Pokud je daný manévr schválen, algoritmus vydá RA, které signalizuje pilotovi UAS jak daný manévr provést. [49]



Obrázek 2 - Schéma funkce algoritmu Stratway, [50]

Algoritmus Stratway pracuje s iteracemi, kdy si algoritmus určí bod A, kde se odchýlí od původního kurzu a bod C, do kterého se po provedení manévr UA opět vrátí. Mezi těmito body iteračně posouvá bod B dále od původní dráhy letu až do doby, kdy je UA v bezpečné vzdálenosti od bodu nejbližšího sblížení. Tento proces je schematicky znázorněn na Obrázku 3.



Obrázek 3 - Způsob iteračního posuvu bodu „B“ algoritmu Stratway, [50]

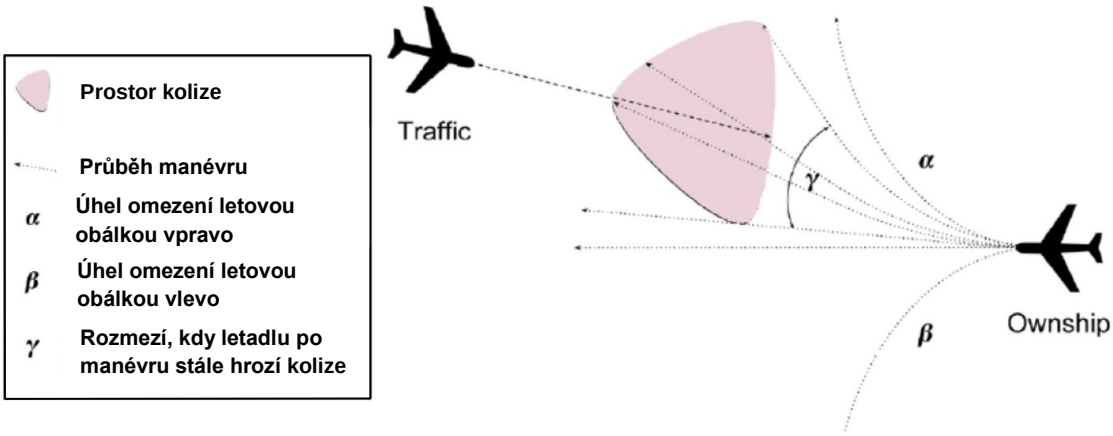
Tento algoritmus byl vyvinut za účelem bezpečnějšího provozu bezpilotních systémů v řízených vzdušných prostorech. Výhodou je, že se systém ADS-B pouze doplní o popisovaný algoritmus, což nevyžaduje složité úpravy UA. Díky tomuto algoritmu by bylo možné výrazně zvýšit bezpečnost leteckého provozu jak letounů bezpilotních, tak i ostatních letadel ve vzduchu. Vzhledem k povinné implementaci systému ADS-B pro všechna letadla ve výše zmíněných vzdušných prostorech a relativně nízké náročnosti na úpravu hardwaru UAS, se mi tento systém jeví jako velmi vhodný pro budoucí použití protisrážkového systému pro UAS. [49]

2.4.3 DAIDALUS

Systém DAIDALUS (*Anglicky: Detect and AvoID Alerting Logic for Unmanned Systems*) je algoritmus, který je alternativním řešením pro Detect and Avoid systémy pro UAS a byl vyvinutý Langleyho výzkumným střediskem NASA (*Anglicky: NASA Langley Research Centre*). DAIDALUS funguje na principu deterministického přístupu [51], kdy algoritmus předpokládá, že popisované veličiny spontánně nemění svůj stav a jsou vázány pevně danými vztahy. Stav tedy není náhodná veličina, ale veličina deterministicky určená vztahy, počátečními podmínkami, okrajovými podmínkami atd. [52] Vztahy jsou zde reprezentovány jako lineární projekce deterministického modelu získané z přehledových palubních systémů, jakými jsou ADS-B nebo radar. DAIDALUS tedy vytváří jakousi simulaci všech pozorovaných cílů, kdy z jejich aktuální konstantní velikosti vektoru rychlosti a směru pohybu, určuje místo, kde se budou cíle nacházet v čase +180 vteřin. DAIDALUS tedy předpovídá místo, kde se budou cíle nacházet za tři minuty a podle toho vyhodnocuje riziko kolize. [51]

Systém je schopný vydat varování definovaná v dokumentu Phase 1 MOPS (*Anglicky: Minimum Operational Performance Standards*). Varování může být dvojího typu. Jednak systém vydá pouze korekční varování v dostatečném časovém předstihu a není nutno provádět prudké manévry. Tento první typ varování bychom mohli přirovnat k vydání TA

(*Anglicky: Traffic Advisory*) u systému ACAS. Druhý typ je pak obdobný s vydáním RA (*Anglicky: Resolution Advisory*), taktéž používaného v systému ACAS, kdy je nutná okamžitá reakce v podobě změny směru letu, aby nedošlo ke kolizi. DAIDALUS sám vypočte nejvhodnější manévr, kterým se kolizi vyhne a jelikož se jedná o bezpilotní systémy, předá tato varování řídící stanici, kde se pilotovi UAS zobrazí, jak úhybný manévr provést. [53] Schéma zobrazující princip funkce systému DAIDALUS je zobrazený na Obrázku 4. DAIDALUS do výpočtu vhodného manévru zahrnuje údaje o výšce, směru, rychlosti letu, ale také třeba údaje o změně vertikální rychlosti letadla. DAIDALUS do svých výpočtů samozřejmě zahrnuje i letové obálky letadla, aby při manévru nedošlo k narušení konstrukce například působením příliš velkých odstředivých sil. [51]



Obrázek 4 - Schéma principu činnosti systému DAIDALUS, [51]

2.4.4 ACAS-Xu

Některé protisrážkové systémy určené pro bezpilotní systémy jsou stále ve fázi vývoje. Příkladem takového systému je i nová generace protisrážkového systému ACAS-X, respektive jeho speciální verze nazvaná ACAS-Xu a určená právě pro využití v UAS. ACAS-X je podle FAA kritickou součástí nezbytnou pro bezpečný provoz systému nové generace (*Anglicky: Next Generation Air Transportation System*), krátce NextGen [54], v oblasti řízení letového provozu. V případě nové verze ACAS-X se předpokládá, že v budoucnu nahradí současný systém TCAS-II [55]. Teď se již zaměřme na speciální verzi určenou pro použití na bezpilotních systémech, tedy na verzi ACAS-Xu. Tato verze systému prošla řadou vylepšení, aby byla schopna plnit požadavky definované Phase 1 MOPS. ACAS-Xu na rozdíl od systému DAIDALUS využívá dynamické programování, analýzu nákladů (z hlavně energetického hlediska) a pravděpodobnostní rozdělení stavů pro výpočet možností, kdy by mohlo dojít ke kolizi mezi UAS s okolním provozem. ACAS-Xu tedy pracuje se stavem a pohybem bezpilotního systému

nedeterministicky neboli stochasticky. [56] To znamená, že algoritmus v některých krocích může volit hned z několika možných postupů, což u deterministického modelu není možné, protože tam je vždy následující krok definován jednoznačně [57]. Systém má definovaný model letadla a jeho senzorů. Tyto modely jsou napojeny na data z přehledových systémů a pomocí nich vytváří rozdělení pravděpodobností pro různé stavy letadla. Tyto pravděpodobnosti jsou poté použity pro výpočet toho, zdali se bude daný objekt nacházet v kolizní trajektorii UA. Pokud ano, modul TRM (*Anglicky: Threat Resolution Module*) použije všechna dostupná data pro zvolení nejvhodnějšího manévru pro odvrácení kolize. [54, 58]

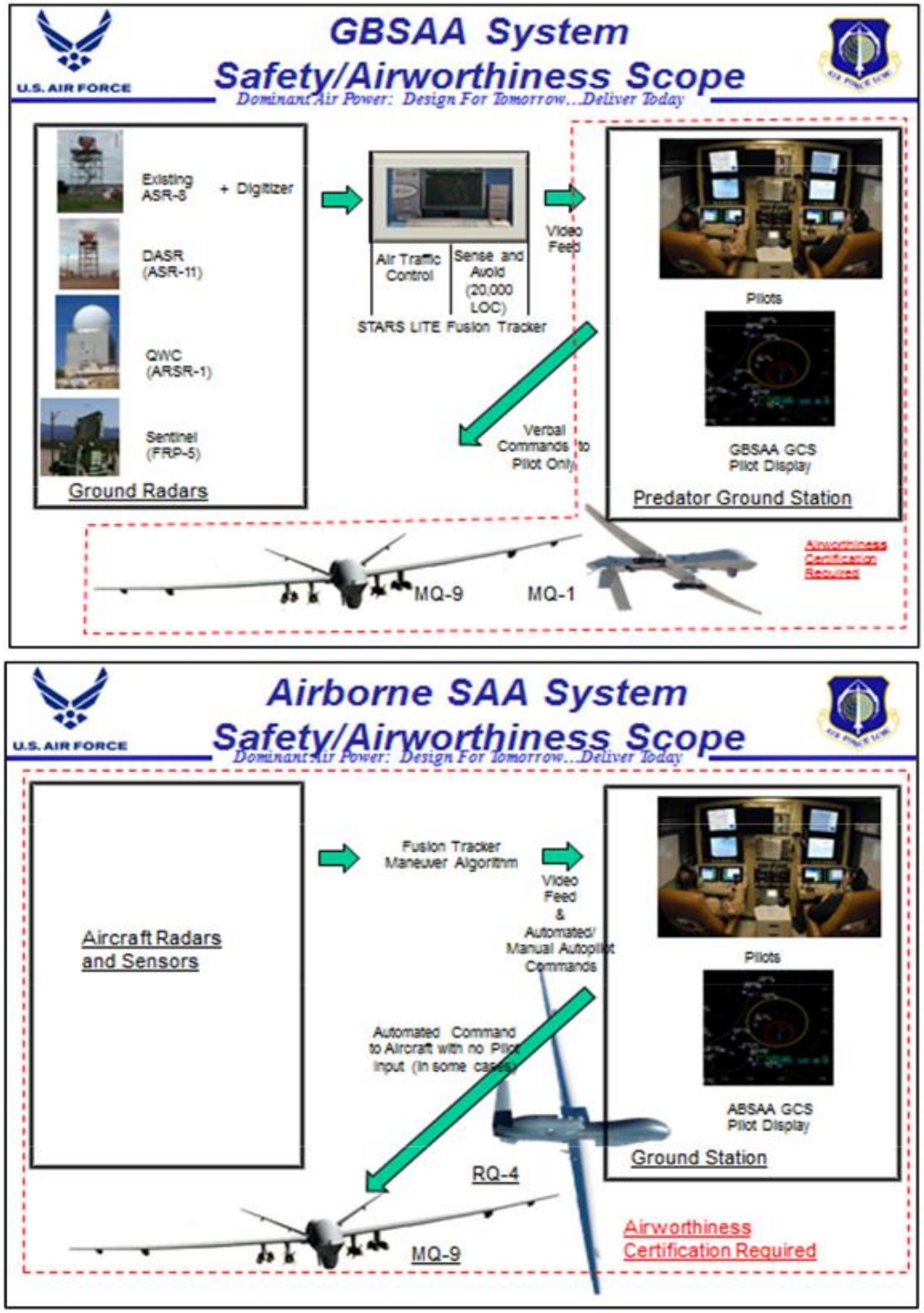
ACAS-Xu, stejně jako jeho předchozí generace, také využívá ke sdělení varování pilotovi RA, kde ho informuje a navádí na správné provedení manévru. Tato generace systému ACAS již vydá pilotovi RA a to, aby provedl úhybný manévr buď v horizontální nebo i ve vertikální ose letu, případně v jejich kombinaci. [54] Osobně si myslím, že v zájmu eliminace možnosti selhání lidského faktoru právě při použití protisrážkových systémů, jakými jsou systém DAIDALUS nebo ACAS-Xu, bude v budoucnu nezbytné, aby tyto systémy pilota v řídící stanici UAS o krizové situaci pouze informovaly a poté zcela autonomně zasáhly do řízení UA a vykonaly tak úhybný manévr. Touto cestou, dle mého mínění, bude manévr vykonán nejpřesněji a tudíž nejbezpečněji. V případě, kdy celý úkon vykonává pilot se může v rámci selhání lidského faktoru přihodit hned několik situací, které mohou následně vést ke kolizi UAS s druhým objektem. Při použití zcela autonomních protisrážkových systémů je, podle mého názoru, naprosto nezbytná komunikace jednotlivých UAS mezi sebou, tak jako je tomu již dnes v případě každodenního používání systému TCAS.

2.4.5 ABSAA

Systém nazvaný jako Airborne Sense and Avoid (ABSAA) je dalším typem systému, který je stále ve fázi vývoji. Na jeho konci bude tento systém plně nahrazovat schopnosti pilotů, kteří na palubách bezpilotních systémů chybí, „detekovat, vycítit a vyhnout“ se případné překážce. Vývoj tohoto systému probíhá již od roku 2001, kdy se postupně vyvíjí vhodné algoritmy a také se zajišťuje správná součinnost ABSAA s různými senzory na palubě UA. Oproti pozemní alternativě – systému GBSAA, je tato „vzdušná“ verze postavená na spolupráci kooperujících objektů. ABSAA sbírá data z palubních senzorů a odpovídačů, jakými jsou například ADS-B nebo TCAS. Tento systém je tedy vyvíjen jednak pro detekci již zmíněných kooperujících cílů, ale také počítá s vybavením UAS různými systémy pro detekci cílů nekooperujících. Zde by šlo zejména o elektro-optické systémy anebo o využití palubního radaru. Schopnost detekovat jak kooperující, tak nekooperující objekty v blízkosti letadla poskytuje systému ABSAA přesný a reálny

obraz situace v okolí bezpilotního letadla. Vývoj systému ABSAA je také nastaven tak, aby jeho finální verze splňovala přísné požadavky od FAA, které definují možnost pohybu UAS v řízených vzdušných prostorech. [59]

Oproti například pozemním systému pro DSA je systém ABSAA plně palubní, a proto je nutná certifikace pro bezpečný provoz právě na palubě UAS, což na celkový vývoj tohoto systému klade nemalé nároky v oblasti spolehlivosti a především bezpečnosti [60]. Armáda Spojených států a letectvo USA úzce spolupracují na vývoji obou systémů GBSAA a ABSAA, protože se počítá s budoucí kooperací obou těchto systémů za účelem ještě zlepšit přesnost, ale také poskytnou jakousi „fail safe“ ochranu pro DSA systém na palubě UAS. [59] Na Obrázku 5 vidíme přehledně v grafickém porovnání systém GBSAA a ABSAA a jejich princip součinnosti s ostatními systémy.



Obrázek 5 - Grafické porovnání systémů GBSAA a ABSAA, [60]

V této kapitole jsou podrobně popsány protisrážkové systémy pro použití v bezpilotních systémech. Jednotlivé protisrážkové systémy jsou zde podrobně sepsané a analyzované. Některé z nich se již v dnešní době využívají, některé jsou zatím stále ve fázi vývoje. Chránit UAS proti hrozbě střetu s terénem nebo jiným letícím objektem je bráno jako absolutní nutnost pro budoucí provoz bezpilotních prostředků v řízených vzdušných prostorech. Tato ochrana je taktéž vyžadována i z důvodu strmého navýšení počtu UAS, které jsou každý rok provozovány po celém světě. Velký důraz a iniciativu

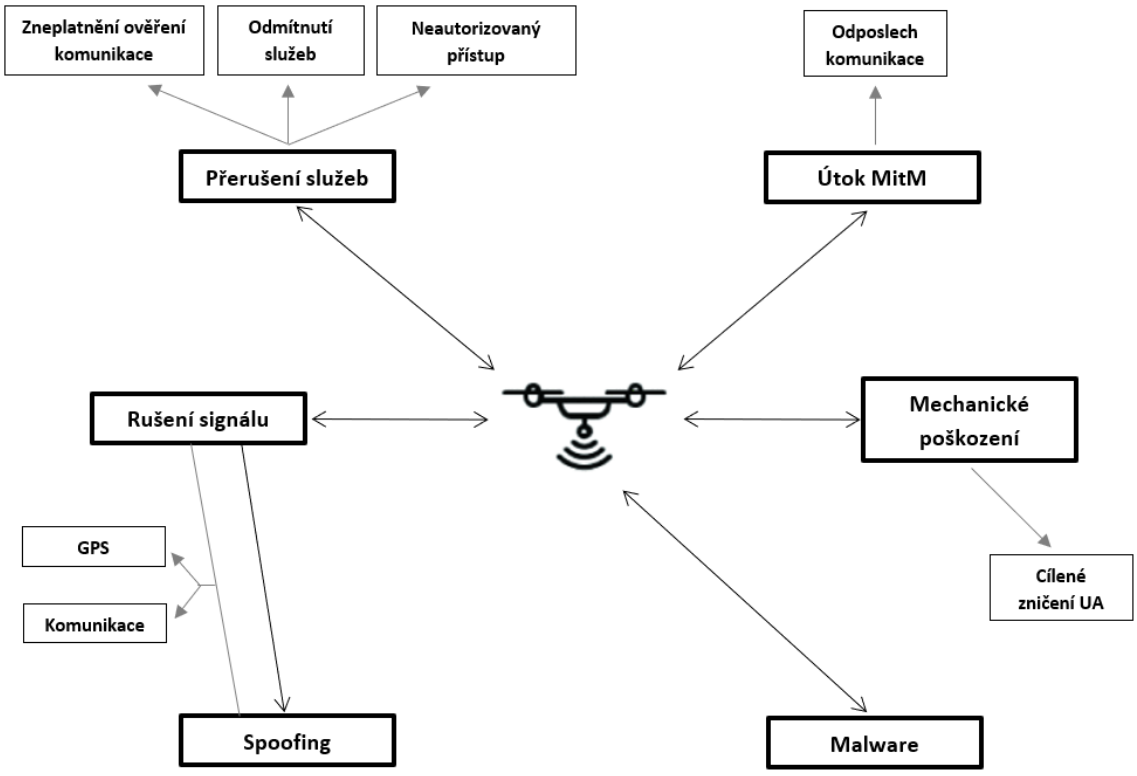
zatím projevují Spojené státy americké spolu s Evropskou unií, které v blízké budoucnosti budou svými zákony přímo vyžadovat použití protisrážkového systému u UAS při jasně definovaných okolnostech. Osobně také vnímám tuto hrozbu jako jednu z největších, hlavně pokud vezmeme v úvahu bezpilotní prostředky určené pro domácí nebo komerční použití, kde je po celém světě tisíce případů srážky UA s cizím tělesem. Zvláště bych kladl důraz na malé UAS, které žádným podobným systémem nedisponují, byť střet takového malého bezpilotního systému často působí nemalé majetkové újmy, či újmy na zdraví. Ve vojenském sektoru je situace odlišná. Vojsko stojí prakticky od počátku za vývojem protisrážkových systémů pro UAS, tudíž lze předpokládat, že jejich UAS disponují alespoň základním protisrážkovým systémem. Nicméně veškeré informace o moderních vojenských UAS nejsou veřejně přístupné z cela logických důvodů, a tak již pravděpodobně vyvíjí další generace protisrážkových systémů, které v budoucnu jistě najdou uplatnění i mimo vojenský sektor.

3 Útoky na komunikační prostředky UAS

Tato kapitola mé bakalářské práce je věnována hrozbám, které mohou UAS ohrozit pro lidské oko neviditelným útokem a samozřejmě se snaží identifikovat nebo navrhnout způsoby, jakými by bylo možné bezpilotní systémy bránit proti útokům právě na jeho komunikační nebo navigační systémy. Bezpilotní systémy pro komerční nebo domácí užívání nejsou na trhu nikterak dlouho, avšak počet útoků směřovaných právě na komunikaci UAS s jeho řídící stanicí nebo „matení“ jeho navigačních systémů se řadí mezi nejčastější typy hrozeb pro UAS. [61] U čistě vojenských bezpilotních systémů patří obrana jejich komunikačních a navigačních systémů k nejdůležitějším zabezpečovacím systémům UAS vůbec. [62] I proto jsou detailnější informace o vybavení vojenských UAS tajné a pro civilní sektor téměř nedohledatelné. To je také důvod, proč bude v této kapitole řeč spíše o bezpilotních systémech pro komerční nebo čistě domácí užívání.

Dnešní UAS jsou schopny zaznamenávat a uchovávat mnoho parametrů o svém letu. Naprostá většina z nich je již schopna pořizovat například kvalitní videozáznam z paluby UA. V blízké budoucnosti se navíc počítá i s použitím UAS jako doručovacího prostředku pro balíčky až ke dveřím jejich adresáta. [63] Všechny zmíněné schopnosti takových bezpilotních systémů z nich dělají poměrně hodnotný cíl zlodějů. Vzhledem k tomu, že UAS v naprosté většině případů startuje a přistává poblíž svého pilota nebo v případě doručování zboží by pravděpodobně přistával již pod dohledem adresáta. Nicméně stále bude existovat pravděpodobnost, že se UA stojící na zemi, pokusí někdo ukradnout. Pokud by tedy došlo k nežádoucí manipulaci s UA stojícím na zemi, navrhoval bych využít již vestavěný reproduktor nebo jím UA vybavit. Tento reproduktor by v případě nežádoucího pohybu vydával sérii zvuků, kterými by své okolí upozorňoval na případnou krádež – tedy byl by zde instalovaný jakýsi alarm. Správné vyhodnocení nežádoucí manipulace se strojem by bylo možné zajistit například tímto způsobem. Pokud by se bezpilotní letadlo pohnulo, což by bylo možné zjistit například díky zabudovaným akcelerometrům, ale nedostávalo by k takovému pohybu žádné příkazy ze své řídící stanice, nebo v případě autonomního letu, kdy by takový pohyb nesouhlasil s letovým plánem UA, by došlo ke spuštění alarmu. Tento alarm by, například u doručovacích UAS, byl aktivní vždy, když se UA nachází na zemi mimo svoji základnu. Poloha základny by byla vyznačena do softwaru UAS pomocí souřadnic. Po jejich dosáhnutí by se pak alarm mohl zcela autonomně vypnout. Druhou možností, která mě napadá, je zabudování RFID (*Anglicky: Radio Frequency Identification*) čtečky přímo do UA. Oprávněná osoba by se pak pro manipulaci se strojem musela vždy pomocí své karty skrze tuto čtečku identifikovat.

Nyní se již zaměřím na ohrožení navigačních a komunikačních systémů, způsobené různorodými útoky, které mohou nastat prakticky při jakékoli části letu a útočník v nich využívá některého komunikačního nebo navigačního systému UAS. Pro přehlednost přikládám schématický obrázek, který je označený jako Obrázek 6, kde je znázorněno hned několik možností, jak lze výše zmíněnými způsoby UAS ohrozit. Postupně tyto hrozby analyzuji a případně navrhnu způsoby, jakými efektivně UAS od těchto hrozeb bránit. Nicméně je důležité zmínit fakt, že schopnost UAS odolat takovým útokům se diametrálně liší u různých typů UAS. To platí vesměs pro všechny způsoby napadení pomocí komunikačních kanálů UAS. Schopnost bránit se takovým útokům je závislá na mnoha aspektech, které velmi často závisí čistě na výrobci UAS. Často se však v softwaru UAS objeví „skulinky“, díky kterým je takový útok možný provést. Vhodnou obranou proti všem takovým útokům se jeví duplikování celého komunikačního systému – to znamená, že celý systém obsahuje dva vysílače a dva přijímače. Díky tomu se tento systém jeví daleko stabilnější a pokud nastane na jednom kanále výpadek, druhý kanál automaticky přebírá kontrolu nad komunikací mezi řídící stanicí a UA. Tímto mezi nimi udržuje stabilní komunikační síť. Dalším důležitým faktorem, jak UAS chránit, je zajistit aktuální verzi jeho softwaru. Protože výrobci často software pro UAS stále vylepšují a vždy nejnovější verze softwaru by měla zajistit co nejnižší pravděpodobnost úspěšného bezdrátového útoku na UAS. [64]



Obrázek 6 - Možné útoky na UAS skrze komunikační systémy, [65]

3.1 Zneplatnění ověření komunikace

Prvním způsobem řadícím se do skupiny útoků, které využívají takzvané „přerušení služeb“ a jakým je cizí osoba schopna ovládnout UA, aniž by s ním přišla fyzicky do kontaktu, je takzvané zneplatnění ověření komunikace mezi řídící stanicí UAS a samotného UA. To znamená, že pilot UA ztrácí díky tomuto útoku veškerou kontrolu nad bezpilotním letadlem. [66] Po takovém útoku by bezpilotní letadlo mělo být k dispozici pro ostatní kompatibilní ovladače, takže pokud by byl útočník takovým ovladačem vybaven, čistě teoreticky, by se mohl k UA připojit a ovládat ho.

Pro takové připojení stačí mít notebook vybavený potřebným softwarem. Díky notebooku se útočník připojí na stejnou síť, na jaké probíhá komunikace mezi UA a jeho pozemní řídící stanicí. Útočník si na zmíněné síti hravě vyhledá MAC (*Anglicky: Media Access Control*) adresu pozemní řídící stanice, díky které se pak velice jednoduše připojí svým ovladačem k UA. Vyhledání MAC adresy není nutné pro jakékoli útoky tohoto typu, nicméně to výrazně urychluje celý proces ovládnutí UA. [67]

Pomocí právě takového útoku může dojít i k fyzickému zničení bezpilotního letounu. Pokud by totiž útočník měl za cíl zničit bezpilotní letoun, má vesměs dva způsoby, jakými to provést. Prvním způsobem je UA fyzicky zneškodnit, to znamená sestřelit nebo jiným obdobným mechanickým poškozením stroj dostat z nebe. Druhým, pro některé případy i jednodušším způsobem pro vykonání takového útoku, je možnost se k bezpilotnímu letounu například výše popsaným způsobem připojit. Poté se dle mého názoru naskýtá hned několik možností, jak ukradený stroj zničit. Osobně bych volil buď střemhlavý let vůči zemi nebo nastavení všech motorů na maximální výkon. Myslím si, že v obou případech je zničení stroje téměř nevyhnutelné. Z logického hlediska se obrany vůči takovému způsobu zničení rovnají schopnostem stroje odolat veškerým útokům na jeho komunikační a navigační systémy, které jsou pospány v této bakalářské práci.

Pro vykonání takového útoku v podstatě stačí využít kupříkladu program „Aircrack-ng“, disponující několika nástroji pro napadnutí připojení Wi-Fi a který je volně dostupný na internetu. Jeden z jeho nástrojů je přímo vyvinutý pro napadení a zneplatnění komunikace mezi vysílačem a přijímačem. Díky známým MAC adresám tento program vyšle balíčky dat, které by měly postačit k přerušení komunikace mezi UA a jeho řídící stanicí. Po tomto přerušení je ovšem těžko předvídatelné, jak se UA zachová. Strojům s méně propracovaným softwarem se pravděpodobně vypnou všechny motory a nezvratně dojde k pádu UA. Naopak stroje s propracovanějšími technologiemi na palubě mohou, po ztrátě signálu ze své řídící jednotky, přejít na záložní komunikační kanál, díky němuž dojde k opětovnému navázání komunikace UA s řídící stanicí.

V neposlední řadě pak může být UA naprogramován tak, aby se při ztrátě signálu vrátil na místo odkud vzlétl a zcela autonomně tam přistál [67]. Zde bych tedy jasně volil UAS, disponující pokročilým komunikačním systémem, který bude výrazně odolnější vůči podobným útokům, než tomu je u méně sofistikovaných UAS. Případně pokud dojde k narušení komunikace mezi UA a jeho řídící stanicí volil bych UAS, který disponuje autonomním systémem pro bezpečné přistání na zem, aby nedošlo k jeho destrukci a aby nedošlo k újmě na zdraví, či poškození věcí třetích osob.

3.2 Odmítnutí služeb

Druhým způsobem přerušení služeb mezi vysílačem a přijímačem UAS je útok nazývaný jako „odmítnutí služeb“. Tento typ útoku se hojně využívá po celém světě, kdy se používá jakožto účelný kybernetický útok nejen na přijímače, ale především obecně na servery všeho druhu. Často je tento útok nazýván jen jako „DoS útok“, z anglického Denial of Services – v češtině tedy odmítnutí služeb. Tento typ útoku tedy vesměs končí také přerušením komunikace mezi částí systému, který byl útoku vystaven, a jeho okolím – tedy stejně jako u předchozího případu [68]. Nicméně útoky typu DoS dosáhnou svého cíle zcela jiným způsobem. Zjednodušeně řečeno, jeden z nejrozsáhlejších typů DoS útoků má za úkol svými dotazy zcela zahltit dotazovaný cíl.

V našem případě tedy opět stačí, pokud si na internetu útočník do svého notebooku nainstaluje jeden z mnoha dostupných programů, který slouží jako generátor paketů a zároveň i jako analyzátor. Tento program poté začne generovat a v rychlém sledu odesílat dotazové pakety ICMP (*Anglicky: Internet Control Message Protocol*), u kterých nečeká na žádnou odpověď. Dotazovaný cíl tyto pakety nestíhá zpracovávat a přehltí se, čímž dojde zároveň k znemožnění jakékoli komunikace do anebo z míněného cíle. Pokud je program vybavený i zmíněným analyzátorem, dochází při útoku k průběžnému vyhodnocování průběhu útoku. V případě potřeby program může automaticky upravit počet vyslaných paketů, případně pozměnit druh paketů tak, aby došlo k co nejúčinnějšímu přerušení komunikace mezi vysílačem a přijímačem. [69]

Pro účinné ochránění bezpilotního systému proti DoS útokům je nutné vybavit jeho komunikační systém speciálním hardwarem. Tento hardware by měl zaručit rozeznání packetů na ty, které jsou součástí komunikace mezi vysílačem a přijímačem a na ty, které jsou součástí DoS útoku. Škodlivé pakety by měly být ignorovány, tudíž by k žádnému přehlcení komunikační sítě nemělo dojít. Je ale nutné dodat, že obsah paketů při útocích DoS se výrazně liší útok od útoku, tudíž při obraně UAS velice záleží na tom, zdali je hardware, případně software schopný rozeznat veškeré i ty nejnovější škodlivé pakety. [70] Zde tedy vidíme jasný příklad toho, proč je nutné udržovat stále aktuální

verzi softwaru UAS, kdy s každou další aktualizací výrobce přidává do databáze další škodlivé pakety, které se mohou při DoS útocích využít. To, do jaké míry je UAS schopný odolat DoS útoku, je vidět na následujícím experimentu, kdy byly dva různé druhy UAS testovány na DoS útoky. U obou bylo nejprve provedeno měření času, který obsahoval dobu zpracování dotazu a jeho cestu k vysílači a zpět, a to při normálním používání, tedy pokud by vše pracovalo tak jak má. U prvního zkoušeného UAS modelu CX-10W, který je miniaturním UAS s cenou okolo jednoho tisíce korun, byla doba odpovědi v průměru 1,8 ms. V průběhu DoS útoku na tento UAS se tato doba odpovědi zvýšila až na 44 ms. To způsobilo problémy v ovládání UA i v jeho přenosu komunikace. Při neustávajícím DoS útoku nakonec došlo ke ztrátě komunikace mezi UA a ovládací stanicí. Bezpilotní letadlo CX-10W se také v průběhu útoku nadměrně zahřívalo. [65]

V druhém případě byl testován UAS Parrot A.R Drone 2.0, který je v průměru cenově 4x dražší než CX-10W. U tohoto modelu byla průměrná doba odpovědi v běžném provozu v průměru 2.3 ms. V době útoku DoS se tato hodnota zvýšila na 20.8 ms. Nicméně po celou dobu útoku zůstala zachována schopnost ovládat UA a tím byla zachována bezpečnost letu. DoS útok se projevil na přenosu obrazu z UA, kdy došlo k viditelnému snížení kvality obrazu. Na UAS Parrot A.R nedošlo k ohřevu vnějšího obalu UA, což poukazuje na lepší odolnost tohoto UAS proti DoS útokům. Důvodem, proč nebyl Parrot A.R Drone 2.0 zasažený DoS útokem tolik jako UAS CX-10W je to, že jeho software obsahuje skript, který disponuje kódem nastavujícím tabulky IP a také definuje jejich jistá pravidla. Jedním z nich je například to, že UAS má ignorovat pakety, které k němu dorazí z jiné MAC adresy, než z kterou je spárovaný. Dále má také omezený počet druhů akceptovatelných paketů, díky čemuž se snižuje šance na zasáhnutí DoS útokem. [65] Výše zmíněné výsledky jasně ukazují na to, že závisí na důmyslnosti softwaru UAS, díky kterému je případný DoS útok zmírněn nebo zcela potlačen. Na druhou stranu je nutné říct, že MAC adresa, ze které je útok veden, může být lehce změněna na falešnou tak, aby si UA myslel, že jde o pakety z jeho párované řídící stanice. Dále musíme brát v úvahu, že šlo pouze o jeden druh DoS útoku, a tak nelze jednoznačně říct, co by se s UAS stalo, kdyby byl proveden další DoS útok s jinými datovými pakety. Tento experiment tedy jasně ukazuje na to, že pokud bude bezpilotní systém vybavený více vrstvami ochrany proti DoS útokům, bude mít zcela jistě větší šanci na překonání takového útoku.

3.3 Neautorizovaný přístup

Posledním způsobem, jakým může být UAS napadnut skrze přerušením jeho komunikačních služeb je útok nazvaný jako neautorizovaný přístup. Jde o přímé spojení útočníka a UA. Útočník nejprve potřebuje udělat „průzkum“ bezpilotního letadla, zdali jsou k dispozici volné porty na UA pro připojení útočníka. Tento průzkum v dnešní době opět zajišťuje volně přístupný program, například Nmap, který po ukončení průzkumu vypíše seznam dostupných otevřených portů. Skrze tyto porty lze posléze vniknout do UA. Toto vniknutí zajistí protokoly, například protokoly FTP (*Anglicky: File Transfer Protocol*) nebo protokoly Telnet. Pokud UAS nedisponuje pokročilým softwarem, který nevyžaduje další ověření takových protokolů, útočník získává přímý přístup do UA. To znamená, že má plnou moc nad tím ovládat stroj a také ihned získává veškerá data a informace, která jsou v dané síti UAS k dispozici. Bez dalšího vybavení ovšem není útočník schopný skrze příkazový řádek UA složitěji ovládat. Nicméně pro získání veškerých dat a případné zničení UA se tento útok jeví jako vhodný. [71]

Obranou proti takovému útoku je opět nezbytné mít software, který disponuje alespoň šifrováním komunikace. Dalším krokem, který může tento typ útoku zcela odvrátit, je vybavit software firewallem, který zajistí ochranu všech portů právě proti vniku neautorizovaných přístupů. Pro úspěšné provedení takového útoku je také nezbytné, aby protokoly, které útočník odešle, nebyly podstoupeny důkladnému ověření. To znamená, že pokud UA neověřuje pravost příchozích protokolů, nemá pak šanci obstát v obraně proti popisovanému útoku. Pro obranu UAS proti těmto útokům tedy stačí instalovat potřebný firewall, který by měl efektivně třídit příchozí protokoly, případně vůbec neposkytnout volné otevřené porty pro navázání další komunikace vyjma té, která je potřeba mezi UA a jeho řídící stanicí. Nicméně i pro tento typ útoku platí, že způsob, jakým se útočník pokusí dostat do UA je velmi individuální, a tudíž stále existuje pravděpodobnost, že i přes veškerá opatření se útočníkovi podaří prolomit firewall a dostat se tak k datům a informacím o UAS.

3.4 Útok MitM

Tento typ útoku nese označení MitM z anglického spojení „Man in the Middle“, které by se dalo volně přeložit jako útok skrze prostředníka. Tímto prostředníkem se myslí samotný útočník, který se dostane do komunikace mezi řídící stanici UAS a její samotný bezpilotní letoun. K provedení popisovaného útoku se dá využít například zařízení Wi-Fi Pineapple. Nejprve útočník uvede zařízení do módu, kdy monitoruje veškeré dostupné přístupové body a klienty, kteří jsou na ně připojeny. Jakmile útočník vybere správný přístupový bod – UA, Wi-Fi Pineapple začne imitovat SSID neboli identifikátor bezdrátové sítě (*Anglicky: Service Set Identifier*), což zapříčiní, že se pilot s řídící stanicí

přepojí z UA do útočníkovo Wi-Fi Pineapple a od té doby má útočník k dispozici veškerou komunikaci mezi UA a jeho řídící stanicí. Útok MitM ještě nebyl podroben žádnému veřejně dostupnému výzkumu, proto nelze jasně určit, co přesně se při takovém útoku odehraje. Teorie je nicméně taková, že by v průběhu útoku měla být zachována spojitá komunikace mezi UA a jeho řídící stanicí a útočník by z počátku měl k dispozici veškerá data a informace o letu. Posléze by bylo jen na útočníkovi, jestli „pouze“ ukradne zmíněná data a v tichosti se z UAS zase odpojí, aniž by o tom pilot UAS věděl, nebo zdali pomocí dalšího hardwaru převezme řízení UA. [72]

Obranou proti útoku MitM je vybavit UAS dostatečně pokročilým softwarem disponujícím spolehlivým firewallem, který by měl podchytit podezřelou aktivitu hned zpočátku a zároveň by měl zajistit ochranu UAS jako celku před takovým útokem. Nevýhodou popisovaného útoku je fakt, že se útočník musí nacházet na místě, kde má dostatečný signál jak od řídící stanice, tak od samotného bezpilotního letounu. Jakmile se totiž jedna ze zmiňovaných částí UAS dostane z dosahu útočníkova zařízení, celý útok je přerušen a celý průběh útoku typu MitM by se musel opakovat.

Proti výše popisovaným útokům se dají nevojenské UAS bránit všemi zmiňovanými způsoby. Pro všechny však platí, že pokud není UA nebo celý UAS vybaven svou vlastní SIM kartou pro nezávislé připojení k internetu, musí být útočník vždy nablízku UA, aby si zajistil dostatečně silný signál relevantních rádiových vln. Jednou z dalších možností, jak tedy UAS bránit proti všem typům útokům na komunikační systémy, je létat v místech, kde by pilot dokázal identifikovat případného útočníka. Tento druh obrany lze využít v přírodě nebo na jiných volných prostranstvích, naopak ve městech nebo při používání UAS nad zástavbou nelze tento typ obrany aplikovat.

U vojenských UAS, které jsou prakticky bez ustání připojeny na internet, jsou dostupnějším, ale také hlavně hodnotnějším cílem jakýchkoli útoků. Informace, technologie nebo samotné vybavení nesené na palubách těchto UAS mají často nevyčíslitelnou hodnotu, a proto by úspěšný útok na takové UAS útočníky byl mimořádně ceněný. Tento fakt se přímo odráží na způsobech obrany vojenských bezpilotních prostředků. K jejich obraně se proto využívají systémy a vybavení lišící se diametrálně od vybavení komerčních nebo civilních UAS. Informace o vybavení vojenských UAS nejsou veřejně dostupné.

I tento fakt zcela jistě můžeme zařadit mezi obranné způsoby, které mají jediný cíl, a to uchovat nejlépe veškeré informace o daném UAS v tajnosti a snížit tak pravděpodobnost prolomení jejich firewallu. Pokud uvážíme prostředí, kde vojenské UAS působí, zjistíme, že se velmi často jedná o odlehlé oblasti, a navíc naprostá většina vojenských bezpilotních systémů operuje v poměrně vysokých výškách. To klade úměrně větší nároky na vybavení potenciálních útočníků, a tudíž tento fakt opět snižuje pravděpodobnost úspěšného útoku na takové UAS.

3.5 GPS jamming

Další systém, který se dnes využívá v mnoha různých odvětvích, je systém pro určení polohy. Jeho celosvětově známé pojmenování GPS vychází z již dříve zmiňovaného anglického sousloví Global Positioning System. Systém GPS však neslouží striktně pro určení polohy přijímače, ale také v některých systémech slouží čistě pro synchronizaci a nastavení správného času v systému. [73] Nejprve tedy krátký úvod k tomuto systému a velice zjednodušený princip funkce GPS.

Díky jeho dostupnosti, a především činnosti, ho tak najdeme v téměř každém bezpilotním systému, vyjma samozřejmě těch úplně nejlevnějších a nejmenších. Tento systém využívá signál přicházející z družic, díky kterému dokáže určit svoji polohu, a to ve všech třech osách. Satelity GPS vysílají data o své pozici a čase. Přijímač z těchto dat posléze dokáže vypočítat svou vlastní polohu. K určení 3D pozice systém GPS potřebuje minimálně signál ze čtyř satelitů. Poté obecně platí, že čím vyšší je počet satelitů, ze kterých je přijímač schopen získat signál, tím vyšší je přesnost určení pozice přijímače. [5] Systém GPS však není jediný systém poskytující polohová data. Dalšími systémy typu GNSS (*Anglicky: Global Navigation Satellite System*) jsou kupříkladu evropský projekt Galileo nebo čínský systém BeiDou, ale i další [7]. Nicméně v současné době je systém GPS nejrozšířenějším typem systému, díky kterému lze určit polohu přijímače prakticky kdekoli na světě. Popisovaný jamming a spoofing je v této práci popsán se zaměřením právě na systém GPS, nicméně v budoucnu se podobné metody cíleného rušení nebo zkreslování dat mohou rozšířit i na ostatní GNSS systémy.

Signál, který přijímač ze satelitu obdrží, musí urazit poměrně velkou vzdálenost, protože tyto satelity obíhají Zemi ve výšce zhruba 20 tisíc kilometrů. Tím vzniká poměrně velký prostor k rušení tohoto signálu. Právě rušení signálu neboli jamming je jedním z případů, jak přijímači GPS zabránit k přijetí signálu ze satelitů, a tím dochází i k zhoršení přesnosti pozičních dat nebo dokonce k úplné ztrátě určení pozice přijímače. Systém GPS využívá k přenosu dat rádiové vlny o známých frekvencích. Zmíněné rušení signálu je založeno na interferenci těchto vln. Skládání neboli interference vln vzniká při střetu dvou vlnění,

které jsou vzájemně fázově nebo dráhově posunuty. Interferenci vln pak ještě posiluje, pokud obě vlnění mají stejnou frekvenci. [13] Při interferenci pak záleží, jak na sebe vlnění narazí. Výsledný kmitavý pohyb vlnění se v různých místech liší. Někde se obě vlny „sečtou“ a zvýší tak výslednou amplitudu, jinde se zase vlny vzájemně utlumí. Mezi rušením a přirozenou interferencí je tedy rozdíl v tom, že rušení je záměrně vyvolaná interference vln, kdy dochází k účinnému rušení signálu díky vhodně vybraným parametrům rušícího vlnění. Výsledkem rušení signálu GPS je většinou kompletní ztráta dat přijímače, který není schopný určit svou polohu. Obrany proti rušení signálu GPS se shodují s těmi, které jsou vhodné jako obrana i v případech, kdy jde o takzvaný GPS spoofing. Tudíž možnosti, jak se bránit rušení GPS signálu, budou uvedeny v kapitole 3.6.1.

3.6 GPS spoofing

Spoofing je anglické slovo vyjadřující podvod nebo jemu podobné klamavé jednání. Tato charakteristika tedy prozrazuje, čím se zabývají následující řádky, tedy jakýmsi klamáním signálu GPS. Aby bylo zmíněné klamání GPS přijímače úspěšné, je nutné k němu vyslat externí rádiové vlny. Ty musí být, jednoduše řečeno, velmi podobné těm vlnám GPS, které přicházejí z družice. Pokud tedy takto útočník synchronizuje originální a klamavé vlnění, přijímač GPS z velké části přijímá právě klamavé vlnění, jelikož je vysíláno s mnohem větší intenzitou než vlnění originální. GPS spoofing může mít za následek zhoršení nebo úplnou ztrátu GPS signálu přijímače, tedy má podobný efekt jako výše popisovaný GPS jamming, nebo může dokonce zajistit, aby přijímač GPS udával špatně svou polohu a co víc, tuto klamavou polohu může útočník dokonce určit dle své libosti. Z toho lze vyvodit poměrně širokou škálu následků, zejména pro systémy jako UAS, kdy je systém GPS mnohdy hlavním systémem určujícím polohu UA v prostoru. Dále je ještě nutné zmínit, že spoofing může zapříčinit okamžité oklamání GPS přijímače nebo se tento účinek může dostavit opožděně a také efekt spoofingu lze častokrát pozorovat i po skončení útoku. [74]

Ze všech výše zmíněných negativních vlivů, které GPS jamming i spoofing způsobují, je zřejmá nutnost ochrany GPS přijímačů proti těmto vlivům. Právě díky poměrně snadnému zkreslení signálu GPS mnohé bezpilotní systémy nevyužívají jako jediný navigační systém GPS, nýbrž častokráte je tento systém doplněn o známý inerční navigační systém. Nicméně řada UAS využívá systém GPS a ve velké míře ho začleňuje jako hlavní systém pro různé vytvoření trasy letu nebo při nouzových situacích, kdy dojde ke ztrátě spojení UA a jeho řídící stanice. V takovém případě se UA může vrátit právě díky GPS systému na předem stanovené místo, kde bezpečně přistane. Takovéto zdvojení navigačního systému se dá zajisté započítat jako preventivní ochrana

navigačního systému UAS před úplnou ztrátou pozičních a jiných letových dat, nicméně inerční navigační systémy nemohou nahradit veškeré možnosti nabízené systémem GPS. Pro GPS jamming a spoofing existuje celá řada ochran. V následujících řádkách jsou tyto ochrany analyzovány a je zhodnoceno jejich možné uplatnění v bezpilotních systémech.

3.6.1 Obrany proti spoofingu a jammingu

Jako jednu z prvních uvedu skutečnost, že systém GPS, jehož základy byly uvedeny do provozu již v sedmdesátých letech minulého století, je v dnešní době, oproti ostatním moderním GNSS systémům, v jistých ohledech zastaralý. Například nový evropský projekt Galileo je již od základu vybaven pokročilým šifrováním svých vysílaných radiových vln. Tyto vlny jsou vybaveny jakýmsi digitálním podpisem daného satelitu Galileo, díky kterým už nebude tak jednoduché aplikovat na systém Galileo spoofing. Výhodou je, že toto šifrování bude k dispozici nejen pro vojenský sektor tohoto systému, ale i pro sektor civilní. Tato obrana tedy úspěšně eliminuje spoofing, nicméně proti jammingu již úspěšná není. Pro systém GPS však takovýto typ obrany již není možný aplikovat, jelikož k jeho zavedení je nutné systém GNSS důmyslně připravit již od jeho vývoje. [75]

Další možností, jak úspěšně bránit bezpilotní systémy proti zkreslujícím nebo dokonce rušícím signálům, je použití antény CRPA (*Anglicky: Controlled Radiation Pattern Antennas*). Ta byla původně vyvinuta čistě pro vojenské účely, nicméně s postupem času se dočkala i uvedení do civilního sektoru. Velikou výhodou CRPA je to, že se nemusí zasahovat do softwaru systému, kam chceme tuto anténu nainstalovat. Jedná se totiž skutečně jen o výměnu antény, která vše potřebné ke své práci již obsahuje. Někdy se tak může stát, že CRPA je o něco větší, něž běžná anténa. CRPA je složena z několika jednotlivých antén, díky čemuž dokáže mapovat prostorovou různorodost signálů, které do antény CRPA přicházejí. Jelikož spoofing i jamming signály jsou útočníkem z pravidla vysílány pomocí přístroje, tedy jsou vysílány z jednoho určitého místa, k CRPA anténě tak tyto signály dorazí z jednoho směru. Zatímco v běžném provozu by měl signál z GNSS systémů přicházet do antény přijímače prakticky ze všech stran stejně, jelikož je tento signál vysílán několika satelity, které se zrovna nacházejí v různém uspořádání ve vesmíru.

Princip fungování antény CRPA je tedy, jednoduše řečeno, filtrování prostorového signálu, který do antény přichází ve větší intenzitě z jednoho určitého směru. Tím dojde k odstranění škodlivého signálu, zatímco slabší, avšak pravý signál je nadále použit pro výpočet polohy přijímače. Velikou výhodou tohoto řešení je účinnost celého zařízení, kdy antény CRPA využívají vojenské síly po celém světě již přes dvacet let. Další nepřekonatelnou výhodou je možnost poměrně snadné aplikace antény CRPA do bezpilotního systému. [76]

Obrovská nevýhoda antény CRPA je její cena a složitost, což se projeví i na celkové ceně bezpilotního systému, který by byl takovou anténou vybaven. Tudíž v civilním sektoru se s anténami CRPA zatím setkáme jen zřídkakdy. Revoluční v tomto směru může být například řešení od jedné izraelské společnosti. Ta v lednu 2019 představila zařízení nazvané Pyramid GNSS™, které snadno schováte do dlaně ruky, tudíž je možno ho bez větších problémů zakomponovat do přijímačů různých GNSS systémů. Velikost současné verze, nazvané V1, v porovnání s budoucí generací označené jako V2, je vidět na Obrázku 7. Byť je toto zařízení teprve novinka, žádost o patent této firmy prozrazuje princip funkce tohoto zařízení. Ten je založen na pluralitě GNSS antén připojených do více GNSS přijímačů. Každá anténa pak disponuje zvláštním materiálem, který pohlcuje radiové vlny. Díky tomuto materiálu má každá anténa dostatečnou citlivost na to, aby určila směr, ze kterého daný signál přichází. Pyramid GNSS™ není schopný pracovat s takovou přesností jako anténa CRPA, nicméně na jednoznačné vyloučení falešného nebo rušícího signálu mu jeho sensibilita stačí. Princip funkce využití několika antén je podobný, jako u antény CRPA, avšak Pyramid GNSS™ je výrazně levnější a menší. Tudíž má velký potenciál obsadit trh s menšími zařízeními, jakými jsou právě i civilní bezpilotní systémy nebo automobily. V blízké budoucnosti pak firma počítá s uvedením ještě menší verze Pyramidu GNSS™, takzvané V2, která by se dala zakomponovat i do mobilních telefonů. Tuto obranu shledávám jako jednu s největším potenciálem pro budoucí využití u UAS, kdy za poměrně malou cenou dostaneme malé, ale účinné zařízení, které dokáže překazit útok vedený jako jamming nebo spoofing na systém GNSS na palubě UA. [77]

Obrázek 7 - Porovnání velikostí Pyramid GNSS™ verzí V1 a V2, [78]

Závěrem celé této kapitoly je nutné podotknout, že s rychlým rozvojem bezpilotních systémů v posledních letech, rapidně stoupá i počet volně dostupných prostředků pro uskutečnění široké škály útoků na komunikační a navigační systémy bezpilotních systémů. Na internetu lze velmi snadno dohledat programy a detailní návody, jak jednotlivé útoky provést. Objevují se zde i plně automatické programy, někdy označované jako malware, které dokážou doslova během několika vteřin proniknout do bezpilotního letounu a kupříkladu mu vypnout všechny motory. Jak jsem zjistil, tento malware je vytvářen ve velkém množství jedinci, kteří hledají chyby v obranách UAS a na jejich základě poté vytváří onen malware. Ve většině případech je ovšem útok limitován na jednu skulinku v obraně UAS a pokud je výrobcem odstraněna, například aktualizací softwaru UAS, je logicky takový malware nepoužitelný.

Na druhou stranu, jak již bylo popsánu výše, na internetu se dají nalézt i komplexnější programy, které dokážou napadnout a případně ovládnout i relativně chráněný UAS. V této kapitole jsou analyzovány i obrany proti takovým útokům. Je poměrně složité konkrétně popsat jednotlivé typy obran, protože se typy útoků stále vyvíjejí a s nimi i dané obrany, nicméně obecně platí, že je nutné mít v UAS co nejaktuálnější software přímo od výrobce UAS, který disponuje velkými finančními prostředky a je v jeho zájmu udržet ochranu svých UAS na vysoké úrovni. Jakožto uživatelé bychom se poté měli

soustředit na ochranu například vlastních chytrých telefonů, pomocí kterých lze dnes ovládat také širokou škálu bezpilotních prostředků určených pro veřejnost. Chytré telefony se totiž také mohou stát terčem útoku nebo do nich může být instalovaný zmíněný malware, skrze který se poté útočník dostane k bezpilotnímu letadlu a všem datům, které obsahuje. Při výběru UAS je v dnešní době nutné dbát na jeho vybavení a důkladně zkontrolovat jeho stupeň šifrování komunikace. I zde platí, čím vyšší stupeň, tím nižší šance, že stroj podlehne některému z útoků. Asi každému je jasné, že u UAS určených pro vojenské účely nebo pro provoz u složek záchranných, či policejních je nutné, aby disponovaly mnohem důmyslnějším systémem schopným daný UAS ubránit. K takovým strojům ovšem není mnoho veřejných informací o jejich vybavení, a tudíž nelze přesně specifikovat stupeň jejich ochrany, nicméně pro úspěšný útok na takto vybavené UAS již v naprosté většině případů nebude stačit software, který je volně dostupný na internetu.

Nicméně výrobci ani uživatelé nesmějí zapomínat na hrozby působící právě na komunikaci mezi řídící stanicí a bezpilotním letadlem, případně na všechny komunikační kanály provozované daným bezpilotním systémem, jež jsou klíčovými systémy pro bezpečný provoz celého UAS. S dalším rozvojem UAS a jejich stále větší dostupností nejen pro veřejnost, ale i pro komerční sektor, se dá očekávat, že útoků právě na komunikační nebo navigační systémy bezpilotních systémů bude přibývat, a proto je a bude nezbytné, aby výrobci věnovali zabezpečení takových komunikačních kanálů vysokou pozornost a bezplatně poskytovali pravidelné aktualizace softwaru pro jejich UAS a co nejvíce tak snížili pravděpodobnost úspěšného útoku na UAS.

4 Fyzické poškození UAS

Pokud analyzujeme hrozby působící na bezpilotní systémy, nesmíme, mimo výše popisované hrozby, opomenout na fyzické neboli mechanické poškození UAS. Takovým způsobem bude samozřejmě bezpilotní systém poškozen i při srážce s jiným objektem ve vzduchu nebo při srážce s terénem. Tento typ hrozby a spojených obran si však vyžádal samostatnou kapitolu. Vše ohledně srážky s letícím objektem, případně srážky s terénem je popsáno v druhé kapitole této bakalářské práce.

Srážka ovšem není zdaleka jediným typem hrozby mechanického poškození UAS, se kterou se v provozu různých typů bezpilotních systémů můžeme setkat. Tato kapitola je tedy zaměřena na několik hrozeb, které reálně bezpilotním systémům hrozí v rámci jejich provozu.

4.1 Sestřelení

V minulosti byla prakticky jedna možnost, jak sestřelit z oblohy letící předmět. Ať šlo o letouny, vrtulníky nebo vzducholodě, zpravidla se používaly k sestřelení buď rakety nebo klasická munice, která na cíli způsobila mechanické poškození neslučitelné s dalším provozem zasaženého objektu bez nutné opravy. Častokráte však byl takový zásah pro stroj zcela fatální a nejdéle při nekontrolovaném nárazu do země došlo k jeho úplnému zničení. V dnešní moderní době toto však již nejsou jediné možnosti, jak sestřelit z oblohy letící objekt, byť je tato metoda stále poměrně spolehlivá. Začněme ovšem s těmito konvenčními způsoby sestřelení.

4.1.1 Konvenční zbraně

V případě sestřelení klasickou municí, například z brokovnice nebo samočinné zbraně, není potřeba tuto metodu hlouběji rozebírat. Je vcelku jasné, že cíl musí být na dohled, aby střelec mohl správně zamířit. Letící objekt by se neměl pohybovat příliš rychle. V případě civilních nebo komerčních bezpilotních systémů je poměrně malá šance, že bude za letu UA sestřeleno právě tímto způsobem. Ve Spojených státech je díky tamním zákonům o zbraních tato pravděpodobnost mírně vyšší, avšak i tak je to velice nepravděpodobné. Proti tomuto útoku existuje prakticky jediná ochrana. S UA se pohybovat rychle anebo dostatečně vysoko, aby střelec, který bude pravděpodobně na zemi, nemohl zamířit. Dnešní civilní/komerční UA jsou poměrně kompaktní, tudíž ještě více znesnadňují sestřelení tímto způsobem. Vojenské UAS jsou samozřejmě díky povaze své činnosti vystaveny mnohonásobně vyššímu riziku sestřelení. Pohybují se ovšem zpravidla ve vyšších letových hladinách, a tudíž je jejich sestřelení prostřednictvím samočinných zbraní ze země také málo pravděpodobné. [14]

Dalším konvenčním způsobem sestřelení je možnost použít rakety vypálené buď ze země nebo ze vzduchu. Tento způsob již zahrnuje širokou škálu možných způsobů, jak raketu na pohybující se cíl navádět. Příkladem může být teplem naváděná střela nebo raketa naváděná pomocí radarové stanice. Tento typ útoku je naopak velmi účinný i na ničení letících objektů ve velkých výškách, a to i při pro poměrně vysokých rychlostech. [79] Na druhou stranu se tato technologie využívá čistě ve vojenském průmyslu, tudíž jsou tyto rakety hrozbou prakticky jen pro vojenské bezpilotní systémy. Musím podotknout, že šance pro sestřelení malého UAS za pomoci naváděné rakety je velmi malá, a to hned z několika důvodů. Malé bezpilotní systémy se pohybují relativně nízko nad zemi a v kombinaci se svou velikostí jsou pro primární radar téměř nezaznamenatelné. Tepelně naváděné střely by se daly využít pro zničení UAS, které jsou poháněny spalovacím motorem, protože i díky vlastní zkušenosti vím, že malé UAS poháněné elektromotory při svém provozu neemitují do okolí extrémní teplo. Dalším důvodem je i to, že se čistě z ekonomického hlediska nevyplatí sestřelit malý a relativně levný UAS pomocí rakety s cenou v řádech stovek tisíc, či dokonce několika milionů dolarů. [80] Aktuální je však sestřelení amerického bezpilotního letounu patřícího pod U.S. Navy, označovaného jako Broad Area Maritime Surveillance (BAMS-D) nebo zkráceně RQ-4A. Šlo o prototyp, který je upravenou verzí známějšího UAS označovaného jako RQ-4 Global Hawk. Sestřelený typ tohoto UAS není vybaven žádnými zbraněmi a slouží čistě pro průzkum a shromažďování informací při letech primárně nad vodními plochami. Tento UAS je schopný letu až do výšky 60 000 stop, což odpovídá asi 18 kilometrům. Je tedy zřejmé, že ke zničení tohoto UAS, s cenou přes 170 milionů amerických dolarů, byla zapotřebí poměrně výkonná raketa. [81] V médiích se uvádí, že za sestřelením tohoto UAS stojí vzdušný obranný systém Iránu Raad. Jde o systém se středně dlouhým doletem raket, schopným sestřelit letoun ve středních a vyšších letových hladinách. Systém Raad, v překladu z perštiny bychom tento systém nazvali „Hrom“, údajně vypustil raketu Sayyad (Lovec) [82] s kombinovaným systémem navigace. Systém Raad je velmi podobný ruskému obrannému systému SA-11 Buk. [83]

O obranách moderních UAS nejsou k dispozici žádné informace, nicméně lze předpokládat, že průzkumná verze RQ-4A není vybavena sofistikovanou ochranou proti sestřelení. Ze zveřejněných záznamů a oficiálních stanovisek totiž není patrné, že by UA aktivoval před sestřelením jakoukoli obranu proti dané raketě. Podle mého názoru by se takto drahé stroje měly vybavit alespoň základní obranou proti tepelně naváděným střelám, známou pod pojmenováním „flares“ neboli světlice. Bezpilotní systémy tohoto typu totiž nejsou schopny prudkých manévrů, a proto nemají proti podobným raketám bez žádné zvláštní obrany příliš velkou šanci. Další možností, jak ochránit bezpilotní

systém proti zničení je vybavit ho technologií známou pod anglickým názvem „stealth“. To znamená vyrobit jeho povrch ze speciálního materiálu, který výrazně snižuje odrazivou plochu radarového záření (*Anglicky: Radar Cross Section – RCS*) a to buď odrazem paprsků tak, aby se nevrátily zpět k radaru nebo jejich pohlcením. Pro pohlcení jsou nejvhodnější RAM materiály (*Anglicky: Radar Absorbent Materials*), které pohlcují a přeměňují radarové záření na tepelnou energii a tím snižují odrazivost letounu [84]. Poslední možností, jak chránit letoun před „očima“ radaru je vybavit ho rušičkou, která vysílá stejný signál, jenž by se od letounu odrazil, ale s opačnou fází. Tímto způsobem dojde k vyrušením obou fází, a tudíž se zpět k radaru nic nevrátí. [85]

4.1.2 Elektromagnetický puls

Nyní se však již dostaňme k těm ne zcela běžným způsobům, pomocí kterých lze také sestřelit létající objekt. Těchto způsobů existuje hned několik a v téměř všech případech jde o poměrně drahé technologie na vývoj a na pořízení, nicméně jejich provoz je oproti například raketám mnohonásobně levnější. [86]

První možností, jak zničit elektroniku v UA, je vyslat cílený elektromagnetický puls (*Anglicky: Electromagnetic Pulse – EMP*). Jde o krátký puls elektromagnetické energie s vysokou intenzitou, který ničí zasažené elektrické obvody. Tyto pulsy mohou být buď člověkem vytvořené, anebo i přírodní. Nicméně ty přírodní nemají, až na výjimky, tak vysokou intenzitu, aby zničili běžné elektrické obvody v UAS. Jako ochrana proti tomuto způsobu útoku je uzavřít obvod do Faradayovy klece. Takovým způsobem budou obvody chráněny před elektrickou složkou pulsu. Pro ochranu proti magnetické složce pulsu je nutné vložení do magneticky vodivé krabice. V aplikaci bezpilotních systémů není ovšem vždy možné, už jen z ekonomických důvodů, aby byly tyto podmínky vždy splněny a bylo tak dosáhnuto kompletního stínění. V každém případě je reálná možnost chránit pouze ty systémy, které jsou životně důležité pro bezpečné přistání stroje. Útok EMP má však i své nevýhody, kdy dokáže vyřadit z provozu veškeré elektrické obvody, které mu přijdou do cesty. Při jeho nevhodném užití tak může dojít k velkým škodám široké veřejnosti, kdy může být zničeno široké spektrum systémů, od rozvodné sítě elektrické energie až po mobilní telefony. [9, 11, 13]

4.1.3 Laser

Další nekonvenční metodou, jak zničit bezpilotní letoun, je možnost využití laseru. Jde o techniku vyslání úzkého proudu fotonů s vysokou mírou energie [86]. Již v roce 2014 proběhly testy amerického zařízení XN-1 LaWS. Tento systém právě pomocí laseru úspěšně zničil jak pozemní cíle, tak i bezpilotní letouny. Konkrétně tyto testy probíhaly z paluby námořní lodě, které v budoucnu budou sloužit jako primární nosič této laserové

zbraně. [87] Použití laseru, kdy paprsek letí rychlostí světla a v případě, že „narazí“ na svůj cíl, začne vystavený materiál rychle tavit – to vše v řádu sekund – se zdá být jako ideální zbraň. A opravdu laserové dělo nemá příliš nevýhod. O jedné nevýhodě se však mluví, je jím počasí, protože některé zdroje uvádí, že laserový paprsek lze poměrně dobře tlumit nebo odrážet od drobných kapek vody. Tedy například při velké oblačnosti nebo hustém dešti by laserové dělo nemuselo být natolik účinné, jako za jasné viditelnosti. [88] Oproti tomu však laserové dělo disponuje hned několika zásadními klady. Prvním je, že jeden „výstřel“ z výše uvedeného děla vyjde přibližně na jeden americký dolar [86]. Další obrovskou výhodou je téměř instantní zasažení cíle, tudíž není nutné při zaměřování počítat s pohybem cíle, balistikou obecně nebo se snášením projektilu větrem. To, že klady převažují zápory laserového děla podporuje i Americké námořnictvo, které si již dvě tato laserová děla závazně objednalo a do služby by se měly dostat kolem roku 2021. [89] I tato zpráva jasně vyjadřuje budoucnost tohoto typu zbraně. Nicméně žádná odborná literatura nehovoří o dostatečně kvalitní obraně proti laserovému dělu. Jisté však je, že dnes běžně používané materiály pro bezpilotní systémy pravděpodobně nebudou dostatečné, aby UA před laserem ochránily.

4.2 Lapení do sítě

Tato hrozba opět není tou pravou hrozbou pro veškeré typy bezpilotních systémů. Lapení bezpilotního letounu do sítě je možné dvěma způsoby. Prvním je možné vystřelení sítě z přenosné nebo napevno umístěné zbraně, kdy se síť po vystřelení při svém letu rozepne do své plné velikosti, „obepne“ svůj cíl, čímž zpravidla vyřadí z činnosti vrtuli nebo vrtule UA, a tím dojde k pádu [90]. Tato zbraň může být instalována i na jiné bezpilotní letouny [91]. Druhou možností je pak umístění sítě svisle, jako závěs pod jiný bezpilotní letoun a následně s ním doslova chytit pronásledovaný stroj [92]. Tento způsob zneškodnění UA je vidět na Obrázku 8. Z obou popisovaných metod lapení do sítě je zřejmé, že takto půjdou zlikvidovat jen stroje, které létají buď tak nízko, aby na ně síť vystřelená ze zbraně doletěla, nebo aby je byl UA se zavěšenou sítí schopný dohonit a polapit. V takovém případě bude jistě pro obsluhu řídící stanice UA s podvěšenou sítí snazší svůj cíl polapit, když na něj bude mít přímý výhled. Lapení do sítě je tak hrozbou primárně pro nízko a pomalu letící UA.

Tato metoda je poměrně účinná, protože jakmile se síť „zamotá“ do rotorů, UA nemá naprosto žádnou šanci se z dané situace dostat. [93] Jedinou obranou proti této hrozbě je schopnost vyhnout se vystřelené síti vhodným úhybným manévrem nebo uniknout pronásledujícímu UA. K těmto manévrům ale musí být pilot poměrně zkušený a mít dobrý rozhled na celou situaci. Pokud ovšem neřídí svůj stroj „na dohled“, nýbrž přes kamerový systém, může snadno přehlédnout střelce nebo onen bezpilotní letoun se zavěšenou sítí.

Obrázek 8 - Lapení UA do sítě za pomoci sítě zavěšené pod větším UA, [94]

4.3 Útok dravého ptáka

Tato kapitola podrobněji analyzuje pro UAS ne příliš častou hrozbu, a to hrozbu od velkých ptáků, především dravců, kteří jsou schopni na bezpilotní prostředek zaútočit, případně ho tak i zneškodnit. Zcela podle logického uvažování se tato hrozba bude týkat zpravidla menších UAS, které by byl schopen dravec zneškodnit, tudíž větší stroje se musí dravce obávat jen v důsledku jeho případného nasátí do motoru. Ve volné přírodě je velmi málo pravděpodobné, že by se na UA znenadání vrhl nějaký dravec, nicméně tyto případy jsou již zdokumentovány.

V naprosté většině se jednalo o bezpilotní letadlo menší velikosti, na které se dravý pták znenadání vrhl a svým útokem UA prakticky zneškodnil a zabránil tak v dalším letu. Takový moment je zachycen na Obrázku 9. Videa z podobných útoků jsou na internetu snadno vyhledatelná a dostupná. A co víc, již v roce 2016 proběhla medii zpráva o tom, že holandští vědci ve spolupráci s místní policií vycvičili několik orlů, kteří uvnitř cvičné haly poměrně spolehlivě likvidovali vznášející se bezpilotní letadla. Počítalo se s tím, že by takto vycvičení dravci mohli v budoucnu chránit zakázané prostory pro let UAS například blízko letišť nebo jiných vládních budov. [95]

Obrázek 9 - Zneškodnění UA dravým ptákem, [96]

Jako obrana proti této poměrně kuriozní hrozbě se nabízí vybavit bezpilotní letoun určitým typem plašičky dravců, která by případný útok mohla odvrátit. Pro potenciální využití takovéto plašičky na UAS jsem vybral dva typy plašiček, které by, dle mého mínění, mohly UAS proti dravcům ochránit. Jedná se o typy plašičky principem založené na vysílání určitých zvuků. Druhým typem by mohla případně být vizuální plašička, která by, buď samostatně nebo ve spolupráci s prvním typem plašičky, dravce úspěšně vyplašila a znemožnila tak poškození UA.

4.3.1 Zvukové plašičky

U tohoto typu plašičky, jak již její označení napovídá, funguje plašení ptáků na základě zvuku, který je produkován plašičkou. V případě útoku dravého ptáka na UAS jsou k dispozici dva druhy zvuků, kterými lze zvíře vyplašit a tím ho přimět, aby svůj útok nedokončilo. Prvním druhem vydávaného zvuku je vytvoření série hlasitých zvuků, které už jen svou akustickou silou dokážou dravce vyplašit. Navíc by v tomto případě šlo o zvuky nepocházející z přírody, ale takzvané zvuky umělé. V dnešní době jsou k dispozici účinné plašící zařízení. Bohužel je naprostá většina z nich pro účely ochrany UAS proti dravcům zcela nepoužitelná. Jedním z mála reálně využitelných řešení je ultrazvukový vysílač. Ultrazvukové frekvence přesahují 20 kHz a jsou tedy pro lidské ucho neslyšitelné, tím by se vyloučila možnost, že by tato plašička dravců mohla způsobit nadměrný hluk v okolí obydlených území nebo jiné problémy spojené s užíváním generátorů hlasitých zvuků. V současnosti existuje již několik výzkumů se zaměřením na otázku, zdali jsou ptáci schopni vnímat ultrazvuk, případně do jakých frekvencí, či nikoli. Závěry těchto výzkumů se však obecně liší pro jednotlivé druhy ptactva. Některé druhy ptactva přestávají slyšet frekvence přesahující 10 kHz. [97] Existující výzkumy samozřejmě nemapují kompletně veškeré žijící druhy ptactva, takže není stoprocentně jasné, zdali by byla ultrazvuková plašička na daného dravce účinná či nikoliv. Pro stoprocentní účinnost by se musely provést experimenty, které by jasně prokázaly schopnost vnímat ultrazvuk nejčastějších volně žijících dravců v dané oblasti.

Nicméně pro použití zvukové plašičky lze využít zvuk zcela jistě slyšitelný pro všechny druhy ptactva – například zvuk imitující výstřel, výbuch nebo další tomu podobný zvuk, který zcela přirozeně dravce vyplaší. Při plašení dosáhneme u ptactva nejlepších výsledků, pokud budou zvuky vydávány nepravidelně a také bude použito několik různých zvuků o více frekvencích. Dále se celková účinnost plašičky zvyšuje tím, že dochází k aktivaci plašičky pouze na krátký časově omezený úsek. Těmito opatřeními se výrazně snižuje šance, že si predátor na zvuky plašičky jednoduše navykne a nebude je již vnímat jako nebezpečí, tudíž již nedojde k jeho vyplašení. [97]

Druhou možností je takzvaná bio-akustika (*Anglicky: bioacoustics*). Bio-akustika je založena na tom, že pracuje se zvuky, které jsou produkovány živými organismy a zároveň tyto zvuky ovlivňují jejich chování. Znamená to tedy naprogramovat zvuk vydávaný plašičkou tak, aby připomínal jakési nouzové volání nebo výstrahu před nebezpečím, které by za normálních okolností vydával jiný dravec. Útočící dravec by tak dostal signál, že jemu také možná hrozí nebezpečí a svůj útok by přehodnotil. Bio-akustika se z vědeckého hlediska jeví jako účinnější pro odpuzování všeho druhu ptactva. Nyní jsou představeny výhody, kterými bio-akustická plašička disponuje. První z nich je vlastnost bio-akustických zvuků mající menší dopad na své okolí, tudíž nejsou především pro lidi příliš do ucha bijící. Tato vlastnost se může hodit především poblíž obydlených oblastí nebo v místech, kde nechceme na letící UAS plašičkou příliš upozorňovat. Další výhodou je, že bio-akustické zvuky mohou být vysílány při nižších intenzitách hlasitosti, oproti „umělým“ zvukům. [10] Nevýhodou bio-akustických zvuků je ovšem to, že každý druh ptactva má „svoji“ řeč, což znamená, že nouzové zvuky vydává každý druh ptactva odlišné od ostatních. Tudíž by se do plašičky muselo nahrát nebo naprogramovat více zvuků od různých druhů dravců. Toto řešení mírně snižuje efektivnost plašičky, protože v reálu se může stát, že na UAS bude útočit druh dravce, kterého žádný z bio-akustických zvuků nezastraší. U plašičky používající bio-akustiku bychom opět měli integrovat systém, který by plašičku spouštěl pouze v daný okamžik. Toto řešení výrazně zvyšuje celkovou účinnost akustických plašiček. Pro celkové zvětšení účinnosti plašiček je ještě vhodné doplnit audio plašičky například o plašičky vizuální. Právě tomuto typu plašiček se věnuje následující kapitola této bakalářské práce. [8]

Jednou z nevýhod celého konceptu audio plašičky je fakt, že na produkci zvuku, který by pokryl dostatečný prostor okolo bezpilotního letounu, je potřeba určitý výkon. Produkce takového výkonu by, především na menších UA, mohla způsobit rychlejší vybití akumulátoru, a tudíž zkrácení jeho letuschopného času. Dále je hned z několika výše uvedených důvodů nutné, aby nebyla audio plašička zapnutá neustále a pokud možno byla v kombinaci s vizuálním odpuzovačem. Dále je třeba, aby bylo možné plašičku na dálku zapínat, respektive vypínat. [98]

4.3.2 Vizuální plašičky

Vizuální plašičky v klasickém slova smyslu nemají ve spojení s bezpilotními systémy reálné využití. Existuje však několik způsobů, které by do koncepce odstrašování dravců pomocí vizuálních plašiček zapadly. Nicméně pouhé umístění vizuální plašičky na bezpilotní letadlo nezajistí stoprocentní jistotu na odehnání dravce touto plašičkou. Stejně jako u zvukových plašiček je velice individuální, zdali se daný dravec nechá

plašičkou zastrašit či nikoli. Dle mého názoru nezáleží jen na druhu dravce, ale i na samotných jedincích, kteří mohou na totožnou plašičku různorodě. V každém případě bych se ale přiklonil k možnosti použití audio-vizuální kombinace plašičky, abychom zajistili co nejúčinnější efekt odstrašení dravce. Vizuální plašičky lze rozdělit na dvě menší skupiny. První skupinou jsou takzvané pasivní vizuální plašičky, které ke své činnosti nevyužívají žádný zdroj energie, a tudíž fungují nepřetržitě. Jde především o speciální typy a vzory nátěrů. Druhou skupinou jsou poté analogicky aktivní vizuální plašičky, které pracují na principu aktivního vyzařování světelných vln.

První možností, jak UAS chránit pasivní vizuální plašičkou, je vyrobit bezpilotní letadlo v takzvaných aposematických barvách, tj. v barvách, které v přírodě obecně značí určité nebezpečí. Jde zde především o výrazné odstíny barev červené, žluté, ale také například modré. Dále je nutné vzít v úvahu, pokud se rozhodneme pro nepoužití aposematických barev, nýbrž pro přírodní maskování bezpilotního letounu, je více než nutné, abychom se vyhnuli kombinaci barev, které by se mohly přiblížit k podobě zbarvení určitého druhu zvěře, které dravec v přírodě přirozeně loví. Aposematické barvy však sami o sobě pravděpodobně cvičeného dravce od útoku na UAS neodradí. [99]

Další možností, jak vybavit UA zvláštním druhem pasivní vizuální plašičky, je využití schopnosti některých druhů ptáků vnímat ultrafialové (*Anglicky: Ultraviolet – UV)* záření. Použitím nátěru, který by trup bezpilotního letounu učinil reflektující UV záření, by se také z části přispělo k tomu, že se bezpilotní letoun dravci při jeho útoku vhodně zaleskne, což způsobí úlek a dezorientaci zvířete. Tato vizuální plašička by pravděpodobně neodradila všechny dravce, nicméně může zvýšit pravděpodobnost úleku predátora. Myslím si, že pokud bude dravec k ničení bezpilotních letadel přímo vytrénovaný, lze jen těžko odhadovat, jakou účinnost by takový nátěr měl. [100] Použití UV nátěru bych tedy využil pouze v kombinaci s ostatními druhy vizuálních plašiček, a to ke zvýšení celkové účinnosti plašení.

Jednou z aktivních vizuálních plašiček je možnost využití sekvence záblesků jasného světla, nejlépe opět aposematických barev, které by mohly oslnit dravce a ochránit tak UA před zneškodněním. Sekvence záblesků, které by vysílaly světlo při různých frekvencích záblesků se jeví jako účinnější než použití jediné frekvence záblesků. Použití tohoto způsobu plašičky má však i svá omezení. Kupříkladu z principu činnosti je jasné, že nejvýhodnější použití takové plašičky je za šera nebo za tmy. Právě tehdy je v okolí totiž nedostatek slunečního záření, a tudíž je i největší šance, že se podaří dravce oslnit a vyplašit. Tato vizuální plašička se výborně hodí do kombinace se zvukovou plašičkou, čímž se zvyšuje šance na úspěšné vystrašení útočícího dravce a tím i odvrácení jeho

útoku. Pro aktivní vizuální plašičky platí pravidlo, že vyžadují poměrně dobré načasování zahájení sekvence záblesků, takže je nutné, aby měl pilot na UA dostatečný výhled a v pravý čas plašičku aktivoval. [101]

Posledním způsobem vizuálního plašení je využití laseru. Principiálně je to obdobné s předchozím případem plašení pomocí jasných záblesků. Využili bychom viditelné spektrum laserového paprsku. Jak zelený, tak červený laser se ve výzkumech jeví jako účinný při plašení různých druhů ptáků. I pro tento způsob aktivního vizuálního plašení platí, aby sepnutí sekvence rozsvěcení laseru proběhlo ve správný čas. Účinnost laserové plašičky se zvýší tím, že frekvence záblesků nebude stálá, ale bude se v čase měnit. U plašičky pomocí laseru navíc vyvstává problém s nutností nasměrování laseru přímo na útočícího dravce, což reálně není za letu proveditelné. [102] Pro tento druh plašičky bych tedy aplikoval možnost instalace několika drobných laserových vysílačů s možností pohybu. Na dané vysílače by byly instalovány optické čočky, které by paprsek nasměrovaly tak, aby byl do okolí šířen v ose kolmé na osu vyzařování laseru. Tímto řešením zvýšíme pravděpodobnost oslnění dravce paprskem díky tomu, že je plocha, kterou laser zasáhne několikanásobně větší než bez použití uvedené čočky. Dohromady se tedy nabízí možnost utvořit pomocí několika pohyblivých laserů, kterými by byl UA vybaven, jakousi laserovou mříž, která by měla podstatně větší pravděpodobnost na úspěch odvrátit útok dravce.

Aktivní vizuální plašičky dravců mají výhodu v tom, že nevydávají žádný zvuk a z tohoto hlediska jsou velmi diskrétní. Jejich použití je však nejúčinnější, pokud je v okolí malé nebo žádné množství světla. Za nevýhodu vizuálních plašiček bych zařadil především to, že záblesky mohou v temném prostředí nechtěně zaujmout především lidi i na vzdálenost několika set metrů, což může být v určitých případech nechtěné.

Pro aktivaci jak zvukových, tak vizuálních plašiček se nabízí vybavit bezpilotní letadlo systémem, který by detekoval dravce autonomně a uměl by plašičky také sám zapínat, respektive vypínat. Toto řešení bych ovšem neviděl jako nejšťastnější, jelikož by na to musel být UAS patřičně vybaven. Musel by disponovat systémem kamer, které by dokázaly sledovat okolí bezpilotního letadla v zorném poli o 360°. Dále by musela být doplněna řídící jednotka UA o software, který by dravce rozpoznal a spustil systém plašiček. Zejména pro menší UA, které jsou potenciálním cílem dravce, by mělo navýšení hmotnosti o kamerový systém zásadní roli jak v doletu, tak v manévrovatelnosti. Nesmíme zapomenout, že software by musel být na vysoké úrovni, aby dokázal rozpoznat dravce útočícího na UA například od prolétajícího ptactva. Pokud by daný software mylně identifikoval hrozbu na UA a spustil oba druhy plašiček

v okamžik, kdy bezpilotnímu letounu nehrozí žádné nebezpečí, mohl by tak na UA upozornit a vystavit ho tak jinému nebezpečí. Právě kvůli převládajícím negativním vlivům tohoto autonomnímu systému, bych se přikláněl spíše ke spouštění plašiček, které by bylo plně v režii pilota UAS.

Dle mého názoru tedy mohou plašičky ve správné kombinaci a správném prostředí fungovat velmi spolehlivě. Z velké části bude záležet na samotném jedinci dravce, jak bude reagovat na danou plašičku. Dále bude hrát velkou roli správné načasování pro zapnutí plašičky, které může výrazně ovlivnit její účinnost. Volbu, zda vybavit UAS těmito plašičkami, bych zvážil podle velikosti daného bezpilotního systému a způsobu jeho budoucího využití. Nesmíme zapomínat, že při zapnutí aktivních plašiček dojde k prudkému nárůstu spotřeby energie, a tudíž musí být jejich aktivace zvláště u UAS poháněných z baterií, dostatečně uvážená a případně aktivována jen v opravdu nezbytné situaci. Pro malé bezpilotní systémy bude zakomponování plašičky samozřejmě náročnější, nicméně malá UAS jsou pro dravce tím cílem, který jsou schopni zneškodnit. Plašička tak může být právě tou ochranou, která pomůže UAS bezpečně dostat do jeho cíle.

5 Přehled hrozeb působících na UAS a jejich obran

5.1 Tabulka pro přehled protisrážkových systémů

Pro přehlednost nyní následuje tabulka všech protisrážkových systému, které jsou v této práci obsaženy. Tyto systémy jsou do tabulky sepsány v takovém pořadí, v jakém se postupně v práci nacházejí. Pro kompletní přehlednost jsou ke každému z těchto systémů vypsány i jejich klady a zápory. Ty jsem vybíral jak na základě literatury, tak na základě vlastního logického uvažování.

Tabulka 1 - Tabulka protisrážkových systémů

Hrozba	Obrana	Typ obrany	Klady	Zápory
Srážka s letícím objektem / srážka se zemí	Protisrážkový systém – Nekooperativní DSA technologie	Radar (SAR)	- Malá velikost - Malá anténa - Možnost vytvořit 3-D SAR - Vhodnější pro stacionární cíle	- Nutný pohyb UA - Zpoždění signálu
		GBSAA	- Využití pozemních radarů (primárních i sekundárních) - Vyhodnocuje konfliktní situace - Spolupráce s ABSAA	- Nutnost min. 3 pozemních radarů - Zatím pouze pro vojenské účely v USA
		Laser	- Schopnost detekovat i malé objekty všeho druhu (ve velkém rozlišení) - Díky možnosti konfigurace za letu má malou chybovost - Nezávadnost pro oči	- Zatím nelze použít na autonomní lety (chybí software)
		Systém pro detekci pohybu	- Vysoká spolehlivost	- Nutnost instalace více kamer
	Protisrážkový systém – kooperativní DSA technologie	ADS-B jako DSA	- Využití stávající sítě ADS-B	- Nutnost palubního odpovídače
		Stratway	- Zohledňuje letovou obálku UA - Součástí je „detektor konfliktů“ – jakési jištění správnosti manévru	- Nutnost drobné konfigurace pro každý typ UAS
		DAIDALUS	- Vydává upozornění na provoz i jasné pokyny pro úhybný manévr - Zohledňuje letové obálky	- Ve vývoji - Vytváří pouze jeden možný úhybný manévr
		ACAS-Xu	- Vytvořen přímo pro UAS - Vytváří několik úhybných manévrů najednou	- Ve vývoji
		ABSAA	- Možnost detekovat kooperující i nekooperující cíle - Možnost spolupráce s GBSAA	- Ve vývoji

5.2 Tabulka pro přehled ostatních hrozeb a obran proti nim

Druhá tabulka obsahuje veškeré zbylé hrozby a obrany proti nim, které jsou obsaženy v této bakalářské práci. Těmito hrozbami jsou útoky na komunikační prostředky bezpilotního systému a různé druhy fyzického poškození UAS. Taktéž tato tabulka obsahuje sloupec s nejvíce ohroženým typem bezpilotního systému pro každou hrozbu.

Tabulka 2 - Tabulka ostatních hrozeb a obran proti nim

Hrozba	Typ hrozby	Obrana
Útok na komunikační prostředky UAS	Zneplatnění ověření komunikace	- Propracovaný a průběžně aktualizovaný software - Záložní kanál pro komunikaci mezi UA a řídící stanicí - V případě ztráty komunikace by měl být UA schopen bezpečně autonomně přistát
	Odmítnutí služeb	- Speciální hardware + software - Udržovat aktuální software - Příjem paketů pouze z jedné MAC adresy
	Neautorizovaný přístup	- UA by nemělo disponovat volnými porty pro připojení - Ověřovat veškeré protokoly přicházející do UA - Šifrování komunikace mezi UA a řídící stanicí - Firewall, jako ochrana portů UA - Udržovat aktuální software a firewall
	Útok MitM	- Pokročilý software - Firewall
	GPS jamming a spoofing	- CRPA anténa - Pyramid GNSS - Kombinace více antén a následná filtrace rušivého signálu
Fyzické poškození UAS – sestřelení	Konvenční zbraně	- Materiály stealth nebo RAM - Využití falešných cílů pro tepelně naváděné střely
	EMP	- Stěžejní elektrické obvody chránit před elektrickou i magnetickou složkou EMP
	Laser	- Materiál odrážející laserové paprsky
Další možnosti fyzického poškození UAS	Lapení do sítě	- Úhybný manévr - Dostatečná výška letu
	Útok dravého ptáka	- Zvukové plašičky - Vizuální plašičky

6 Vlastní návrh konfigurace vybavení fakultního UAS

Šestá kapitola mé bakalářské práce se věnuje vlastnímu návrhu konfigurace vybavení nebo bychom mohli říct obran jednoho z ústavních bezpilotních systémů. Daný typ UAS je popsán níže. Nejprve budou definovány činnosti nebo způsob využití bezpilotního systému v rámci jeho provozování na Fakultě dopravní Českého vysokého učení technického v Praze, přesněji na Ústavu letecké dopravy. Předpokladem je, že budou tento stroj využívat především studenti, případně zaměstnanci ÚLD. Dále se musí počítat s tím, že ne všichni, kdo budou se strojem létat, umí v dostatečné kvalitě ovládat daný bezpilotní systém. Fakultní UAS tedy bude sloužit zpravidla vždy k zalétání nových studentů tak, aby se správně a intuitivně naučili ovládat daný bezpilotní systém. Dále bude tento UAS pravděpodobně sloužit k dalším cvičným letům studentů nebo zaměstnanců. S ohledem na vybavení UA je pravděpodobné, že pokud bude disponovat dostatečně kvalitní kamerou, bude tento UAS využíván k fotografování nebo natáčení všeho druhu. Zmíněnou kameru by mohli studenti využívat i pro pozorování nebo zkoumání různých hůře dostupných prostor. V neposlední řadě by pak UAS mohl být využíván pro testování zařízení všeho druhu ať už studenty nebo i zaměstnanci ústavu.

Ze všech popsaných činností, pro které bude daný UAS na Fakultě dopravní využíván, jsem vybral jeden model bezpilotního systému. Ten je, dle mých informací, již na ÚLD k dispozici. Je jím DJI Phantom 3 Standard. Jedná se o kvadrokoptéru, tudíž je Phantom 3 schopen vertikálních startů i přistání. Hmotnost bezpilotního letadla je dle výrobce 1216 gramů a velikost je 350 mm, měřeno diagonálně bez vrtulí. Velikostně se tedy rozhodně nejedná o žádný mikro UAS, ale stále je tato velikost možná pro provoz v relativně malých prostorech nebo dokonce k vnitřnímu užívání. Pokud se však bude tento bezpilotní systém využívat venku, jeho maximální výška letu činí 6000 metrů. Navigační systém zde poté poslouží jen GPS. [103] Lépe šifrovaný GLONASS zde není k dispozici. U novějšího modelu – Phantom 4 – je k dispozici i systém GLONASS. [104] Tento UAS tedy není tak dobře chráněn z pohledu spolehlivosti zachovat si správné údaje o své poloze. DJI Phantom 3 je tedy poměrně nechráněný vůči GPS jammingu. Stejně tak v případě GPS spoofingu, kdy nejsou u tohoto modelu instalovaná žádná obranná opatření vůči této hrozbě. Lze předpokládat, že si čip pro příjem GNSS signálu vybere silnější signál GPS, který bude ovšem poskytovat nesprávné údaje. Ve vzduchu poté Phantom 3 Standard vydrží zhruba 25 minut. Tato doba se ovšem může velice lišit v závislosti na teplotě, větru i stylu letu. [103]

K maximálnímu využití všech funkcí tohoto UAS je nutné si do tabletu nebo do smartphonu stáhnout oficiální aplikaci DJI GO. Skrze tuto aplikaci se promítají data letu, obraz a další různé informace. Pomocí této aplikace se dá celý UAS také ovládat. Nicméně z vlastní zkušenosti vím, že ovládání bezpilotního systému čistě skrze chytrý mobilní telefon může, zvlášť začátečníkům, působit mírné obtíže. DJI ovšem k tomuto modelu nabízí i dálkové ovládání s nímž je ovládání UA o poznání jednodušší a intuitivnější. DJI Phantom 3 Standard a jeho dálkové ovládání vidíme na Obrázku 10. Zde je třeba podotknout, že součástí UAS není mobilní telefon, který je taktéž na obrázku vyobrazený. Nicméně výrobce počítá s používáním chytrých telefonů, a proto je tomu uzpůsobena i konstrukce dálkového ovládání. Dále je nutné říct, že dálkové ovládání pro DJI Phantom je schopné pracovat na frekvencích mezi 5.725 – 5.825 GHz, kdy si ovladač při zapnutí sám vyhodnotí, na jaké frekvenci bude přenos probíhat v závislosti na rušivých vlnách přítomných v jeho okolí. [103]

Obrázek 10 - DJI Phantom 3 Standard s dálkovým ovládáním, [108]

Na první pohled je patrná obrovská přednost tohoto UAS a tím je kamera, která je schopna pořizovat záznamy ve 2.7K rozlišení, tedy 2704 x 1520 pixelů s rozlišením 12 MP s 3osou stabilizací [105]. Za nevýhodu tohoto modelu bychom mohli uvést absenci pokročilého protisrážkového systému. DJI Phantom 3 Standard disponuje pouze dvěma kamerami. První slouží ke stabilizaci letu a druhá čistě pro pořizování fotek, či videí [106]. Jeho nástupce DJI Phantom 4 PRO má k dispozici o další tři kamery navíc, které využívá již zabudovaný protisrážkový systém. Ten pochází přímo od výrobce UAS,

který garantuje detekci stacionárních překážek před, za i vedle UA. Nelze však s jistotou říct, jak by se tento systém zachoval v případě letící překážky. Dá se však předpokládat, že pokud by byla překážka dostatečně velká, pak je šance, že by se jí Phantom 4 PRO vyhnul. [107] Byť se nejedná o žádný typ protisrážkového systému popsaného v této bakalářské práci, je tento základní anti kolizní systém prvním krokem pro postupné zavádění podobných systémů i do dalších běžně dostupných UAS. Bohužel model, který je k dispozici na ÚLD nemá tento protisrážkový systém. Vzhledem k povaze činnosti tohoto stroje by byl ideálním doplněním vybavení tohoto UAS pro lety pilotů začátečníků nebo pro lety v stísněných prostorech, například v prostorách školy. Toto byl základní přehled vybavenosti ústavního bezpilotního systému. Samozřejmě se nejedná o kompletní seznam vybavení, nýbrž jen o část, která reprezentuje již zabudované ochrany tohoto bezpilotního systému.

Nyní se ještě zaměřím na extra vybavení, které bych pro tento model UAS doporučil vzhledem k jeho definovanému poli budoucí působnosti. Pokud bychom chtěli, alespoň hodně částečně, vybavit tento UAS nějakým typem protisrážkového systému, ze všech zmiňovaných v této bakalářské práci se mi jeví jako vhodný jeden z nekooperativních protisrážkových systémů, protože se tento UAS bude pohybovat v prostředí, kde s velkou pravděpodobností nebude většina objektů vybavena odpovídačem sekundárního radaru, či jiným podobným vybavením. Z těchto nekooperativních DSA technologií by bylo nejlepší instalovat systém, který využívá k detekci lasery. Tento systém volím jednak s ohledem na velikost, kdy by několik laserů zabralo, dle mého mínění, méně místa než například několik kamer, jako je tomu u Phantom 4 PRO. Zadruhé, jak již víme, laser je schopen detekovat poměrně malé objekty různých tvarů, což z něj činí ideálního kandidáta na protisrážkový systém. A za třetí ke své činnosti nepotřebuje spolupracovat s dalšími systémy, například s radary, které nejsou schopny malé letící objekty vůbec zaznamenat. Systém laserů by se dal také doplnit ještě infračervenými senzory, které by také hlídaly vzdálenost UA od ostatních předmětů. Na druhou stranu, abychom mohli tento bezpilotní systém provozovat bezpečně i v řízených vzdušných prostorech, bylo by nezbytné nainstalovat na něj odpovídač sekundárního radaru. Tím by byla zajištěna ochrana stroje právě při letech ve vyšších letových hladinách nebo při činnosti například v blízkosti letiště. Samozřejmě k takovému provozu nestačí pouze odpovídač sekundárního radaru, ale pilot a stroj musí splnit veškeré, zákonem dané požadavky. Nicméně právě odpovídač sekundárního radaru zajistí viditelnost UA na obrazovkách řídících letového provozu, kteří díky němu znají přesnou polohu UA.

Asi velmi těžko bychom vlastními silami nějak vylepšovali obranu proti útokům na komunikační systémy UAS. DJI jakožto jeden z předních výrobců civilních bezpilotních systémů pravidelně aktualizuje software pro všechny vyrobené UAS tak, aby vždy zajistil ochranu před aktuálními hackerskými hrozbami. Asi bychom těžko konkurovali této společnosti s vývojem vlastní obrany, jelikož DJI sbírá data o svých UAS téměř z celého světa a také se dá předpokládat, že DJI disponuje zkušenými zaměstnanci, kteří se danou problematikou denně zabývají. [109] Dále bych však využil zařízení Pyramid GNSS™, které by bezpilotní systém dokázalo ochránit před GPS spoofingem i jammingem. Výhodou je kompaktnost tohoto zařízení, tudíž by výrazně neomezilo UAS v běžném provozu.

Velice těžko by se dal DJI Phantom 3 Standard vybavit nějakou ochranou proti sestřelení. Navíc stroj používáný v rámci ÚLD se téměř se stoprocentní pravděpodobností nikdy nesetká s takovou hrozbou, proto není v této aplikaci takové obrany potřeba. Naopak společnost DJI nabízí produkt nazvaný DJI Goggles. Jde o brýle pro virtuální realitu, se kterými máte výhled, jako byste seděli přímo v UA. Jde tedy o zařízení, které podstatně zvyšuje rozhled z UA a celkově zlepšuje přehlednost situace ve vzduchu. [110] Tyto „brýle“ by se daly použít jako potenciální zvýšení ochrany proti lapení UA do sítě. Jak již bylo řečeno, téměř jedinou obranou proti tomuto útoku je vhodně načasovaný úhybný manévr, který by díky DJI Goggles mohl být snadněji a lépe proveden. Tuto obranu by však fakultní UAS v běžném provozu opět pravděpodobně nevyužil. Zde ovšem není vyloučeno, že by mohl být využit pro testování dané obrany právě pomocí popisovaných brýlí. DJI Goggles také bezpochyby zlepšují celkovou orientaci pilota, proto by pro něj mělo být snazší UA ovládat a pořizovat například fotky přesně daného objektu i z relativně malé vzdálenosti.

Naopak by DJI Phantom 3 Standard mohl poměrně dobře sloužit jako nosič pro zvukové i vizuální plašičky ptactva. S jeho velikostí disponuje poměrně značným prostorem, kam případné plašičky umístit. Především se jedná o konstrukci, na kterou UA dosedá při přistání. Zde by šly umístit oba typy plašiček. Jako vizuální plašičku bych volil aktivní zábleskova světla, umístěna po jedné na každé straně tak, aby svými záblesky co možná nejvíce osvětlovala celý prostor okolo UA. Jako zvukovou plašičku bych zvolil výkonný reproduktor.

Zde by bylo potřeba experimentu, který by jasně určil počet reproduktorů na UA, jelikož je těžké odhadovat počet potřebných reproduktorů na pokrytí dostatečného prostoru kolem bezpilotního letadla. Jak již víme, UAS může přijít do styku s dravcem prakticky kdykoli, tudíž se daná obrana na UAS hodí. Je ovšem na povážení, jaká je pravděpodobnost daného útoku. Nicméně tento typ obrany by se dále dal využít jako odpuzovač ptactva na letištích, kdy by byl instalován na UAS, které by dané letiště před ptáky za pomoci plašiček chránil.

Závěr

Cílem této bakalářské práce bylo poskytnout přehledný souhrn hrozeb, které působí na civilní i vojenské bezpilotní systémy a současně k těmto hrozbám vytvořit odpovídající seznam použitelných obran. Účelem bylo důkladně se seznámit s danou problematikou ohrožení bezpilotních systémů hned několika možnými způsoby i s metodikou, která se uplatňuje při návrhu jejich obranného vybavení.

Část práce tedy podrobně popisuje jednotlivé možnosti ohrožení UAS, se kterými při své činnosti daný bezpilotní systém přijde do styku. Ke každé hrozbě je poté přiřazen a popsán vhodný způsob, jak daný UAS proti takové hrozbě efektivně bránit. Bylo analyzováno, jakými způsoby lze bezpilotní systém ohrozit a v jakých případech je která obrana vhodnější pro úspěšné odvrácení hrozby.

V úvodních kapitolách bakalářské práce je čtenář obeznámen s principem funkce bezpilotních systémů a také se základními pojmy nezbytnými k pochopení tématu. V médiích se totiž velmi často používají pojmenování, které nejsou uvedeny v žádných nařízeních, či zákonech a čtenář pak není přesně informován o dané problematice.

Podstatná část práce je věnována protisrážkovým systémům. Ty jsou dnes součástí i velkého množství civilních UAS, určených čistě pro domácí využití. Tyto systémy výrazně napomáhají nezkušeným pilotům v ovládání stroje ve stísněných prostorech, ale i ve volné přírodě. Osobně protisrážkové systémy vnímám do budoucna jako podstatnou část vybavení bezpilotních systémů, jelikož pro bezpečnost letového provozu, zejména v řízených prostorech, bude potřeba jejich nezbytná aplikace.

Druhou oblastí představující široké pole možností ohrožení bezpilotních systémů, je útok skrze bezdrátovou komunikaci UAS. V současné době již existuje hned několik veřejně dostupných postupů, jak ovládnout bezpilotní systém. Je nutné podotknout, že se zatím naštěstí jedná především o jednoduché, levné typy UAS. Ty vyspělejší ovšem mohou takovým útokem utrpět poškození, která se projeví na vlastnostech letu nebo komunikaci s řídící stanicí. Do budoucna je nezbytné, aby se bezpilotní systémy chránily dostatečným stupněm obrany proti tomuto typu útoku.

Další skupinou ohrožení bezpilotního systému je jeho fyzické poškození. Zde se nejedná jen o sestřelení konvenčními zbraněmi, ale také například za pomoci laseru. Ten je oproti konvenčním zbraním mnohdy přesnější a zpravidla pak výrazně levnější na provoz. Mezi hrozby fyzického poškození jsem započítal i lapení do sítě, které se dnes často aplikuje pro zneškodnění menších bezpilotních letadel. Poslední podkapitolou je pak útok dravce

na bezpilotní letadlo. Existuje totiž šance, že v přírodě na bezpilotní letoun zaútočí dravec sám od sebe, ale v Evropě se také testuje možnost využití cvičeného dravce, který by měl za úkol chránit vzdušné prostory před malými bezpilotními systémy například v okolí vládních budov nebo v okolí letišť.

Pro celkově lepší přehlednost veškerých hrozeb a obran proti nim jsou ke konci práce vytvořeny dvě tabulky. První se věnuje pouze jedné hrozbě a tou je střet s terénem nebo jiným letícím objektem. V tabulce jsou přehledně zpracovány veškeré protisrážkové systémy popsané v této práci a ke každému z nich jsou ještě pro lepší pochopení a porovnání uvedeny jejich jednotlivé klady a zápory. Druhá tabulka poté shrnuje veškeré zbylé hrozby a příslušné obrany. Obě tabulky jsou vypracovány zcela samostatně a mají sloužit jako stručný přehled těch vůbec nejzákladnějších hrozeb a jako výčet možných aplikovatelných obran proti nim.

V samém závěru práce je popsána možná konfigurace obran pro jeden bezpilotní systém. Typ UAS byl zvolen Phantom 3 Standard od společnosti DJI, který patří Ústavu letecké dopravy na Fakultě dopravní ČVUT v Praze. Konfigurace obranného vybavení je volena vzhledem k budoucímu využití UAS, kterým bude především zácvik nových pilotů, fotografování, pozorování a případně i možnost testování různých systémů pocházejících od studentů fakulty. Některými obrannými systémy již tento model disponuje z výroby, jiné by se musely ještě dodatečně nainstalovat.

Je třeba říci, že k vojenským bezpilotním systémům je k dispozici jen málo informací, které velmi často pocházejí z neověřených, a tudíž neoficiálních zdrojů. Je proto těžké posoudit, jakými technologiemi jsou dnešní nejmodernější vojenské UAS vybaveny. Naproti tomu, u civilních bezpilotních systémů je jejich vybavení snadno dohledatelné. Výrobci se vzhledem k počtu prodaných UAS pro civilní využití stále snaží jejich stroje vylepšovat a instalují do nich velmi moderní a pokročilé technologie.

V budoucnu tak můžeme čekat ještě strmější nárůst počtu bezpilotních systémů, které budou provozovány nad našimi hlavami a je tudíž nezbytné klást velký důraz na stupeň jejich ochranného vybavení. Útočníci jsou téměř vždy o krok napřed, a proto bude nezbytné zakomponovat do vybavení bezpilotních strojů například obrany uvedené v této bakalářské práci. Toto odvětví se však stále vyvíjí a každý rok jsou na trh uvedeny nové technologie jak pro ochranu UAS, tak i pro jejich zničení. Domnívám se, že téma mé bakalářské práce naráží na problematiku, která bude v budoucnu rozsáhle probírána i v nadnárodní politice.

Psaní této bakalářské práce pro mě shledávám jako velmi přínosné. Seznámil jsem se s problematikou ohrožení bezpilotních systémů, ale také jsem si rozšířil znalosti o několik možností, jakými lze tyto systémy chránit. Taktéž doufám, že tato práce v budoucnu pomůže ostatním studentům pro nastudování alespoň části dané problematiky ohrožení a ochránění bezpilotních systémů.

Použité zdroje

Literatura

[1] AUSTIN, Reg. *Unmanned aircraft systems: UAVs design, development and deployment*. Chichester: Wiley, 2010. AIAA education series. ISBN 978-047-0058-190.

[2] BARNHART, Richard K. *Introduction to Unmanned Aircraft Systems*. Boca Raton, FL: CRC Press, 2012. ISBN 14-398-3520-9.

[3] BEARD, Randal W. a Timothy W. MCLAIN. *Small unmanned aircraft: Theory and Practice*. Princeton, N.J.: Princeton University Press, 2012. ISBN 978-0-691-14921-9.

[4] CHAMAYOU, Grégoire. *A Theory of the Drone*. New York: The New Press, 2015. ISBN 1595589759.

[5] EL-RABBANY, Ahmed. *Introduction to GPS: the Global Positioning System*. 2nd ed. Boston, MA: Artech House, 2006. ISBN 978-1596930162.

[6] HAMAN, Tomáš. *Přehled bezpilotních letounů*. Brno, 2010. Bakalářská práce. Vysoké učení technické v Brně. Vedoucí práce Ing. Ivan Dofek.

[7] HOFMANN-WELLENHOF, B., Herbert LICHTENEGGER a Elmar WASLE. *GNSS--global navigation satellite systems: GPS, GLONASS, Galileo, and more*. New York: Springer, c2008. ISBN 978-321-1730-126.

[8] JEREMOVIC, Renata. *Bioacoustical Scaring Trials*. Universitz of New England, New South Wales, Australia, 1990.

[9] KLIMEŠ, Bohdan a Josef Bartoloměj SLAVÍK. *Elektromagnetické vlny*. Praha: Státní nakladatelství technické literatury, 1958. 144248.

[10] KROODSMA, Donald E., Edward H. MILLER a Henri OUELLET. *Acoustic communication in birds*. New York: Academic Press, 1982. ISBN 978-012-4268-012.

[11] LEKNER, John. *Theory of Electromagnetic Pulses*. Morgan & Claypool Publishers, 2018. ISBN 978-1-6432-7019-7.

[12] MARSHALL, Douglas M., Richard K. BARNHART, Eric SHAPPEE a Michael MOST. *Introduction to unmanned aircraft systems*. Second edition. Boca Raton, 2016. ISBN 978-148-2263-930.

[13] SADIKU, Matthew N.O. *Principles of Electromagnetics*. 4th edition. UK: Oxford University Press, 2009. ISBN 019806229X.

[14] WHITTLE, Richard. *Predator: the secret origins of the drone revolution*. New York: Henry Holt and Company, 2014. ISBN 978-0-8050-9964-5.

Elektronické zdroje

[15] VISINGR, Lukáš. *Bezpilotní vzdušné prostředky* [online]. Lvisingr.czweb.org, 2007 [cit. 2019-07-25]. Dostupné z: http://webcache.googleusercontent.com/search?q=cache:p9thPFQdXEoJ:lvisingr.czweb.org/stazeni/atm/uav.rtf+historie+UAV&cd=9&hl=cs&ct=clnk&gl=cz&lr=lang_cs

[16] Co je to bezpilotní letadlo, bezpilotní systém, model letadla? *Úřad pro civilní letectví* [online]. [cit. 2019-06-27]. Dostupné z: http://www.caa.cz/letadla-bez-pilota-na-palube/co-je-to-bezpilotni-letadlo-bezpilotni-system-model-letadla

[17] CORRIGAN, Fintan. *Drone Gyro Stabilization, IMU And Flight Controllers Explained* [online]. 27. srpen 2018 [cit. 2019-02-01]. Dostupné z: https://www.dronezon.com/learn-about-drones-quadcopters/three-and-six-axis-gyro-stabilized-drones/

[18] ČESKÁ REPUBLIKA. *Doplněk X – Bezpilotní systémy*. Praha, 2017, ročník 2017. Dostupné také z: https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-2/data/effective/doplX.pdf

[19] CARPENTER, Paul. *Radio control gear explained* [online]. [cit. 2019-01-22]. Dostupné z: https://www.rc-airplane-world.com/radio-control-gear.html

[20] CLYNCH, James R. *A Short Overview of Differential GPS* [online]. Naval Postgraduate School, prosinec 2001 [cit. 2019-04-22]. Dostupné z: https://www.oc.nps.edu/oc2902w/gps/dgpsnote.html

[21] Example: Automotive Radar Tracking Systems. *Advanced Solutions Nederland BV* [online]. [cit. 2019-04-22]. Dostupné z: http://www.advsolned.com/example_radar_tracking.html

[22] ČESKÁ REPUBLIKA. *Předpis L 6: Zkratky a symboly*. Praha, 2016, ročník 2016, 40-A. Dostupné také z: https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-6/L-6i/data/effective/zkratky%20a%20symboly.pdf

[23] CRAIGI. *Basics of Radio Frequencies for FPV Quadcopter Drones* [online]. 17. listopad 2014 [cit. 2019-02-05]. Dostupné z: https://www.droneflyers.com/basics-radio-frequencies-fpv-quadcopter-drones/

[24] LAFAY, Mark. *Understanding How Your Drone Is Controlled* [online]. [cit. 2019-02-01]. Dostupné z: https://www.dummies.com/consumer-electronics/drones/understanding-how-your-drone-is-controlled

[25] CORRIGAN, Fintan. *How Do Drones Work And What Is Drone Technology* [online]. 26. červen 2019 [cit. 2019-07-02]. Dostupné z: https://www.dronezon.com/learn-about-drones-quadcopters/what-is-drone-technology-or-how-does-drone-technology-work/

[26] Drones: What are they and how do they work? *BBC news* [online]. 31. leden 2012 [cit. 2019-02-05]. Dostupné z: https://www.bbc.com/news/world-south-asia-10713898

[27] How do drones overcome latency? In: *Aviation Stack Exchange* [online]. 29. září 2015 [cit. 2019-02-05]. Dostupné z: https://aviation.stackexchange.com/questions/21352/how-do-drones-overcome-latency

[28] *FAA Releases 2016 to 2036 Aerospace Forecast* [online]. FAA, 24. březen 2016 [cit. 2019-02-07]. Dostupné z: https://www.faa.gov/news/updates/?newsId=85227

[29] FAA. *FAA Aerospace Forecast* [online]. 2018 [cit. 2019-03-19]. Dostupné z: https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2018-38_FAA_Aerospace_Forecast.pdf

[30] *Unmanned Aircraft System (UAS) Service Demand 2015-2035: Literature Review and Projections of Future Usage, Version 0.1*. [online] U.S. DEPARTMENT OF TRANSPORTATION, Cambridge, MA 0214, USA, 2013, [cit. 2019-02-07] Dostupné z: https://fas.org/irp/program/collect/service.pdf

[31] OLIVEROS, Edgardo V. a A. Jennifer MURRAY. *Modeling and Simulation of an UAS Collision Avoidance Systems* [online]. 2010 [cit. 2019-02-07]. Dostupné z: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20100042541.pdf

[32] HOTTMAN, S.B., K.R. HANSEN a M. BERRY. *Literature Review on Detect, Sense and Avoid Technology for Unmanned Aircraft Systems* [online]. září 2009 [cit. 2019-02-11]. Dostupné z: http://www.tc.faa.gov/its/worldpac/techrpt/ar0841.pdf

[33] UNITED STATES OF AMERICA. Right-of-way rules: Except water operations. In: *14 CFR*. 2004, § 91.113, číslo 118334. Dostupné také z: https://www.law.cornell.edu/cfr/text/14/91.113

[34] ROSENKRANS, Wayne. Detect, Sense and Avoid (Expanded Version): Safety forum unravels clues to how unmanned aircraft systems could gain less-restricted access to U.S. airspace. *AeroSafety World* [online]. červenec 2008 [cit. 2019-02-07]. Dostupné z: https://flightsafety.org/aerosafety-world/past-issues/aerosafety-world-july-2008/detect-sense-and-avoid-expanded-version/

[35] What is Synthetic Aperture Radar (SAR)? *Sandia National Laboratories* [online]. [cit. 2019-06-25]. Dostupné z: https://www.sandia.gov/radar/what_is_sar/index.html

[36] REIGBER, Andreas, Fabrizio LOMBARDINI, Federico VIVIANI, Matteo NANNINI a Antonio MARTINEZ DEL HOYO. Three-dimensional and higher-order imaging with tomographic SAR: Techniques, applications, issues. *2015 IEEE International Geoscience and Remote Sensing Symposium (IGARSS)* [online]. IEEE, 2015, 2915-2918 [cit. 2019-06-25]. DOI: 10.1109/IGARSS.2015.7326425. ISBN 978-1-4799-7929-5. Dostupné z: http://ieeexplore.ieee.org/document/7326425/

[37] TANEJA, Narinder a Douglas A. WIEGMANN. Analysis of Mid-Air Collisions in Civil Aviation. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* [online]. 2016, 45(2), 153-156 [cit. 2019-06-25]. DOI: 10.1177/154193120104500233. ISSN 1541-9312. Dostupné z: http://journals.sagepub.com/doi/10.1177/154193120104500233

[38] UNITED STATES OF AMERICA. *Report to Congress on: Unmanned Aircraft Systems Collaboration, Demonstration, and Data Sharing*. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistic, 2014, 1-E04DADA. Dostupné také z: https://www.hsdl.org/?view&did=757204

[39] US Army completes test of GBSAA radar-based system for UAS. *ARMY Technology* [online]. 15. květen 2016 [cit. 2019-03-14]. Dostupné z: https://www.army-technology.com/uncategorised/newsus-army-completes-test-of-gbsaa-radar-based-system-for-uas-4893450/

[40] Ground-based system helps UAVs avoid collisions: New radar system enables unmanned aircraft to see and avoid other aircraft. *MIT Lincoln Laboratory* [online]. Massachusetts, 10. leden 2018 [cit. 2019-03-14]. Dostupné z: https://www.ll.mit.edu/news/ground-based-system-helps-uavs-avoid-collisions

[41] JAMES, Anthony. Testing of GBSAA radar-based system for UAS 0. *Aerospace Testing International* [online]. 20. květen 2016 [cit. 2019-03-14]. Dostupné z: https://www.aerospacetestinginternational.com/news/drones-air-taxis/testing-of-gbsaa-radar-based-system-for-uas.html

[42] SABATINI, Roberto, Alessandro GARDI, Subramanian RAMASAMY a Mark A. RICHARDSON. A Laser Obstacle Warning and Avoidance system for Manned and Unmanned Aircraft: treaties and international agreements registered or filed and recorded with the Secretariat of the United Nations. *2014 IEEE Metrology for Aerospace (MetroAeroSpace)* [online]. IEEE, 2014, 616-621 [cit. 2019-02-28]. DOI: 10.1109/MetroAeroSpace.2014.6865998. ISBN 978-1-4799-2069-3. Dostupné z: http://ieeexplore.ieee.org/document/6865998/

[43] HOTTMAN, S.B., K.R. HANSEN a M. BERRY. *Literature Review on Detect, Sense and Avoid Technology for Unmanned Aircraft Systems* [online]. září 2009 [cit. 2019-02-28]. Dostupné z: http://www.tc.faa.gov/its/worldpac/techrpt/ar0841.pdf

[44] ZHAI, Yun a Mubarak SHAH. Visual attention detection in video sequences using spatiotemporal cues. *Proceedings of the 14th annual ACM international conference on Multimedia - MULTIMEDIA '06* [online]. New York, New York, USA: ACM Press, 2006, 815- [cit. 2019-02-28]. DOI: 10.1145/1180639.1180824. ISBN 1595934472. Dostupné z: http://portal.acm.org/citation.cfm?doid=1180639.1180824

[45] KIMBALL, John W. The Compound Eye. *Kimball's Bilogy Pages* [online]. 17. duben 2014 [cit. 2019-02-28]. Dostupné z: http://www.biology-pages.info/C/CompoundEye.html

[46] ARTEAGA, Ricardo, Robert KOTCHER, Moshe CAVALIN a Mohammed DANDACHY. *Application of an ADS-B Sense and Avoid Algorithm* [online]. srpen 2016 [cit. 2019-03-28]. Dostupné z: https://vigilantaerospace.com/wp-content/uploads/2016/08/Application-of-an-ADS-B-Sense-and-Avoid-Algorithm_AFRC-E-DAA-TN30918_20160007770.pdf

[47] *RTCA DO-282: Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance – Broadcast*. Revision B [online]. 2011. Dostupné z: https://qaget.info/?q=rtca+do+260b+pdf&spid=qslfvbcz4b0qelqf3k4b&sub_id=media

[48] UNITED STATES OF AMERICA. *Advisory Circular: Airworthiness Approval of Automatic Dependent Surveillance - Broadcast (ADS-B) Out Systems*. U.S. Department of Transportation, 2010, s. 20-165. Dostupné také z: https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC%2020-165.pdf

[49] HAGEN, George, Ricky BUTLER a Jeffrey MADDALON. *Stratway: A Modular Approach to Strategic Conflict Resolution* [online]. NASA Langley Research Center, Hampton, Virginia, 23601, USA, 2011, 20. září 2011, (20110015827) [cit. 2019-03-28]. Dostupné z: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110015827.pdf

[50] ARTEAGA, Ricardo, Robert KOTCHER, Moshe CAVALIN a Mohammed DANDACHY. *Application of an ADS-B Sense and Avoid Algorithm* [online]. American Institute od Aeronautics and Astronautics [cit. 2019-03-28]. Dostupné z: https://vigilantaerospace.com/wp-content/uploads/2016/08/Application-of-an-ADS-B-Sense-and-Avoid-Algorithm_AFRC-E-DAA-TN30918_20160007770.pdf

[51] MUNOZ, César, Anthony NARKAWICZ, George HAGEN, Jason UPCHURCH, Aaron DUTLE, Maria CONSIGLIO a James CHAMBERLAIN. DAIDALUS: Detect and Avoid Alerting Logic for Unmanned Systems. *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)* [online]. IEEE, 2015, 5A1-1-5A1-12 [cit. 2019-03-07]. DOI: 10.1109/DASC.2015.7311421. ISBN 978-1-4799-8940-9. Dostupné z: http://ieeexplore.ieee.org/document/7311421/

[52] PŘIBYLOVÁ, Lenka. *Deterministické modely* [online]. In: Brno: Fakulta informatiky Masarykovy univerzity, 2015, 13. listopad 2015 [cit. 2019-03-07]. ISSN 1802-128X. Dostupné z: https://is.muni.cz/do/rect/el/estud/prif/ps15/determ/web/docs/deterministonline.pdf

[53] MUNOZ, César, Aaron DUTLE, Anthony NARKAWICZ a Jason UPCHURCH. Unmanned Aircraft Systems in the National Airspace System:A Formal Methods Perspective. In: *SIGLOG news* [online]. ACM Special Interest Group on Logic and Computation, 2016, s. 67-76 [cit. 2019-03-07]. ISSN 2372-3491. Dostupné z: http://siglog.hosting.acm.org/wp-content/uploads/2016/07/siglog_news_9.pdf

[54] MANFREDI, Guido a Yannick JESTIN. *An Introduction to ACAS Xu and the Challenges Ahead* [online]. srpen 2016 [cit. 2019-03-07]. Dostupné z: https://hal-enac.archives-ouvertes.fr/hal-01638049/document

[55] *Introduction to TCAS II* [online]. U.S. Department of Transportation, 28. únor 2011 [cit. 2019-03-07]. Dostupné z: https://www.faa.gov/documentlibrary/media/advisory_circular/tcas%20ii%20v7.1%20intro%20booklet.pdf

[56] Airborne Collision Avoidance System X. *Massachusetts Institute of Technology* [online]. Lincoln Laboratory, 244 Wood Street, Lexington, MA, 02420, 2015 [cit. 2019-03-07]. Dostupné z: https://apps.dtic.mil/dtic/tr/fulltext/u2/a625750.pdf

[57] Definition of nondeterministic in English. In: *Lexico, Powered by Oxford* [online]. [cit. 2019-03-07]. Dostupné z: https://www.lexico.com/en/definition/nondeterministic

[58] DAVIES, Jason T. a Minghong G. WU. *Comparative Analysis of ACAS-Xu and DAIDALUS Detect-and-Avoid Systems* [online]. NASA Langley Research Center, Hampton, VA 23681-2199, 2018, únor 2018 [cit. 2019-03-07]. Dostupné z: https://www.aviationsystemsdivision.arc.nasa.gov/publications/2018/NASA-TM-2018-219773.pdf

[59] UNITED STATES OF AMERICA. *Report to Congress on: Unmanned Aircraft Systems Collaboration, Demonstration, and Data Sharing*. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistic, 2014, 1-E04DADA. Dostupné také z: https://www.hsdl.org/?view&did=757204

[60] LESTER, Ted, Steve COOK a Kyle NOTH. USAF Airborne Sense and Avoid (ABSAA) Airworthiness and Operational Approval Approach. *Mitre Technical Report* [online]. Bedford, Massachusetts, 31. leden 2014, (1.) [cit. 2019-03-19]. Dostupné z: https://www.mitre.org/sites/default/files/publications/usaf-airborne-sense-avoid-13-3116.pdf

[61] WINKLER, Stephanie, Sherali ZEADALLY a Katrine EVANS. *Privacy and Civilian Drone Use: The Need for Further Regulation* [online]. 2018, (vol. 16, 5), 72-80 [cit. 2019-04-27]. DOI: 10.1109/MSP.2018.3761721. ISSN 1540-7993. Dostupné z: https://ieeexplore.ieee.org/document/8490190/

[62] NORTHRUP, Samuel. New Army vehicles being developed to counter modern threats. *U.S. Army* [online]. 1. duben 2019 [cit. 2019-06-07]. Dostupné z: https://www.army.mil/article/219567/new_army_vehicles_being_developed_to_counter_modern_threats

[63] First Prime Air Delivery. In: *Amazon Prime Air* [online]. 2016 [cit. 2019-04-27]. Dostupné z: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011

[64] MALKA, Natanel. The Latest in Drone Security – How to Protect Your UAV from Data Hacking. *SkyHopper* [online]. 31. srpen 2018 [cit. 2019-04-27]. Dostupné z: https://www.skyhopper.biz/drone-security/

[65] WESTERLUND, Ottilia a Rameez ASIF. Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things. *2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)* [online]. IEEE, 2019, 1-10 [cit. 2019-04-27]. DOI: 10.1109/UVS.2019.8658279. ISBN 978-1-5386-9368-1. Dostupné z: https://ieeexplore.ieee.org/document/8658279/

[66] MILLIKEN, Jonny, Valerio SELIS, Kian Meng YAP a Alan MARSHALL. Impact of Metric Selection on Wireless DeAuthentication DoS Attack Performance. *IEEE Wireless Communications Letters* [online]. 2013, (vol. 2, 5), 571-574 [cit. 2019-04-27]. DOI: 10.1109/WCL.2013.072513.130428. ISSN 2162-2337. Dostupné z: http://ieeexplore.ieee.org/document/6574904/

[67] CORRIGAN, Fintan. How To Secure Your Drone From Hackers Permanently. *DroneZon* [online]. 14. listopad 2015 [cit. 2019-04-27]. Dostupné z: https://www.dronezon.com/learn-about-drones-quadcopters/how-to-protect-your-drone-from-hackers-permanently/

[68] KWON, Young-Min, Jaemin YU, Byeong-Moon CHO, Yongsoon EUN a Kyung-Joon PARK. Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles. *IEEE Access* [online]. 2018, (vol. 6), 43203-43212 [cit. 2019-04-28]. DOI: 10.1109/ACCESS.2018.2863237. ISSN 2169-3536. Dostupné z: https://ieeexplore.ieee.org/document/8425627/

[69] How a 'denial of service' attack works. *CNET* [online]. 14. říjen 2005 [cit. 2019-04-28]. Dostupné z: https://www.cnet.com/news/how-a-denial-of-service-attack-works/

[70] WEISMAN, Steve. What are Denial of Service (DoS) attacks? DoS attacks explained. *Norton by Symantec* [online]. [cit. 2019-04-28]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html

[71] Intrusion detection in wireless ad-hoc networks. *Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom '00* [online]. New York, New York, USA: ACM Press, 2000, 275-283 [cit. 2019-06-07]. DOI: 10.1145/345910.345958. ISBN 1581131976. Dostupné z: http://portal.acm.org/citation.cfm?doid=345910.345958

[72] AGARWAL, Mayank, Santosh BISWAS a Sukumar NANDI. Advanced Stealth Man-in-The-Middle Attack in WPA2 Encrypted Wi-Fi Networks. *IEEE Communications Letters* [online]. 2015, (vol. 19, 4), 581-584 [cit. 2019-06-08]. DOI: 10.1109/LCOMM.2015.2400443. ISSN 1089-7798. Dostupné z: http://ieeexplore.ieee.org/document/7031876/

[73] How Common is GPS Jamming? (And How to Protect Yourself). *Orolia* [online]. 19. březen 2018 [cit. 2019-06-11]. Dostupné z: https://www.orolia.com/resources/blog/jeremy-onyan/2018/how-common-gps-jamming-and-how-protect-yourself

[74] Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure. *National Cybersecurity & Communications Integration Center and National Coordinating Center for Communications* [online]. [cit. 2019-06-12]. Dostupné z: https://www.navcen.uscg.gov/pdf/gps/Best%20Practices%20for%20Improving%20the%20Operation%20and%20Development%20of%20GPS%20Equipment.pdf

[75] OBERHAUS, Daniel. Europe Has Its Own GPS Satellites, and They're More Secure than America's. *Motherboard TECH by VICE* [online]. 14. únor 2017 [cit. 2019-06-13]. Dostupné z: https://www.vice.com/en_us/article/9agw97/europe-has-its-own-gps-satellites-and-theyre-more-secure-than-americas

[76] JONES, Michael. Anti-jam technology: Demystifying the CRPA. *GPS World* [online]. 12. duben 2017 [cit. 2019-06-13]. Dostupné z: https://www.gpsworld.com/anti-jam-technology-demystifying-the-crpa/

[77] Pyramid GNNS. *Regulus: Cyber Defense for Sensors* [online]. 2019 [cit. 2019-07-14]. Dostupné z: https://www.regulus.com/solutions/pyramid-gnss/

[78] DIVIS, Dee Ann. Petite New Spoofing Detector Aims to Protect GPS/GNSS Receivers in Drones, Vehicles — Even Cell Phones. *Inside GNNS* [online]. 7. leden 2019 [cit. 2019-07-25]. Dostupné z: https://insidegnss.com/petite-new-spoofing-detector-aims-to-protect-gps-gnss-receivers-in-drones-vehicles-even-cell-phones/

[79] ASHISH. How Do Guided Missiles Work? *Science ABC* [online]. 2016 [cit. 2019-06-30]. Dostupné z: https://www.scienceabc.com/innovation/how-guided-missiles-work-guidance-control-system-line-of-sight-pursuit-navigation.html

[80] AIRCRAFT PROCUREMENT, Air Force. FY 2011 Budget Estimates. In: *United States Air Force* [online]. Volume I. 2010 [cit. 2019-06-30]. Dostupné z: https://web.archive.org/web/20120304052331/http://www.saffm.hq.af.mil/shared/media/document/AFD-100128-072.pdf

[81] LAW, Tara. Iran Shot Down a $176 Million U.S. Drone. Here's What to Know About the RQ-4 Global Hawk. *Time* [online]. 2019, 20. červen 2019 [cit. 2019-06-30]. Dostupné z: https://time.com/5611222/rq-4-global-hawk-iran-shot-down/

[82] TAGHVAEE, Babak. On: *Twitter* [online]. [cit. 2019-06-30]. Dostupné z: https://twitter.com/BabakTaghvaee/status/1141642879938584577

[83] ROGOWAY, Tyler. Everything We Know About Iran's Claim That It Shot Down A U.S. RQ-4 Global Hawk Drone. *The Drive* [online]. 2019, 20. červen 2019 [cit. 2019-06-30]. Dostupné z: https://www.thedrive.com/the-war-zone/28613/everything-we-know-about-irans-claim-that-it-shot-down-a-u-s-rq-4-global-hawk-drone

[84] SWAYAM, Arora a Ramanpreet KAUR. Stealth Technology And Counter Stealth Radars: A Review. *Nternational Journal Of Engineering And Science* [online]. India: Baddi University of Emerging Sciences & Techonologies, 2013, (Vol. 3) [cit. 2019-07-08]. ISSN 2278-4721. Dostupné z: http://www.researchinventy.com/papers/v3i12/D0312015019.pdf

[85] BERKA, Tomáš. Stealth včera dnes a zítra. *Válka.cz* [online]. 16. březen 2004 [cit. 2019-07-08]. Dostupné z: https://www.valka.cz/newdesign/v900/clanek_10600.html

[86] GETTINGER, Dan. What You Need to Know About Lasers. *Center for the Study of the Drone at Bard College* [online]. 10. listopad 2014 [cit. 2019-06-30]. Dostupné z: https://dronecenter.bard.edu/what-you-need-to-know-about-lasers/

[87] SEIDEL, Jamie. US Navy orders laser cannon to be mounted on active warship within a year. *News.com.au* [online]. 26. březen 2019 [cit. 2019-06-30]. Dostupné z: https://www.news.com.au/world/us-navy-orders-laser-cannon-to-be-mounted-on-active-warship-within-a-year/news-story/b4cd491f15edaa4e8d6708fb07bc42c5

[88] SOLODOV, Alexander, Adam WILLIAMS, Sara Al HANAEI a Braden GODDARD. *Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilit* [online]. 2017 [cit. 2019-06-30]. Dostupné z: https://www.osti.gov/servlets/purl/1356834

[89] BRUCE, Robert. The US Navy's Electric Weaponry. *Small Arms Defense Journal* [online]. 19. únor 2016 [cit. 2019-06-30]. Dostupné z: http://www.sadefensejournal.com/wp/the-us-navys-electric-weaponry/

[90] DONOVAN, Alexander. Drone Hunters: 9 of the Most Effective Anti-Drone Technologies for Shooting Drones out of the Sky. *Interesting Engineering* [online]. 22. leden 2019 [cit. 2019-07-01]. Dostupné z: https://interestingengineering.com/drone-hunters-9-of-the-most-effective-anti-drone-technologies-for-shooting-drones-out-of-the-sky

[91] COXWORTH, Ben. DroneCatcher drone-netting drone gets an upgrade. *New Atlas* [online]. 18. červen 2018 [cit. 2019-07-01]. Dostupné z: https://newatlas.com/dronecatcher/55056/

[92] WILLIAMS, Rhiannon. Tokyo police are using drones with nets to catch other drones. *The Telegraph* [online]. 11. prosinec 2015 [cit. 2019-07-01]. Dostupné z: https://www.telegraph.co.uk/technology/2016/01/21/tokyo-police-are-using-drones-with-nets-to-catch-other-drones/

[93] SkyWall 100. *OpenWorksEngineering* [online]. 2019 [cit. 2019-07-01]. Dostupné z: https://openworksengineering.com/skywall-100/

[94] BLOOMBERG. The rise of drones: Can nations control the spy in the sky?. *The Japan Times* [online]. 19. leden 2016 [cit. 2019-07-25]. Dostupné z: https://www.japantimes.co.jp/news/2016/01/19/business/tech/rise-drones-can-nations-control-spy-sky/

[95] ONG, Thuy. Dutch police will stop using drone-hunting eagles since they weren't doing what they're told: Who could have predicted this was a bad idea? *The Verge* [online]. 12. prosinec 2017 [cit. 2019-01-15]. Dostupné z: https://www.theverge.com/2017/12/12/16767000/police-netherlands-eagles-rogue-drones

[96] REUTERS. Drone Defense Startups Flock to the Rescue. *Fortune* [online]. 21. březen 2017 [cit. 2019-07-25]. Dostupné z: https://fortune.com/2017/03/21/drone-defense-companies/

[97] FITZGERALD, S. *Managing Bird Damage in Crops* [online]. Ontario Fruit and Vegetable Growers Association, květen 2013 [cit. 2019-01-15]. Dostupné z: https://onvegetables.files.wordpress.com/2013/06/managing-bird-damage-in-crops-factsheet-final.pdf

[98] AVERY, Michael L. a Scott J. WERNER. Frightening Devices. *USDA National Wildlife Research Center - Staff Publications* [online]. University of Nebraska, 2017 [cit. 2019-01-15]. Dostupné z: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=2991&context=icwdm_usdanwrc

[99] KALMBACH, E. R. a J. F. WELCH. Colored Rodent Baits and Their Value in Safeguarding Birds. *The Journal of Wildlife Management* [online]. 1946, (vol. 10, 4) [cit. 2019-01-15]. DOI: 10.2307/3796245. ISSN 0022541X. Dostupné z: https://www.jstor.org/stable/3796245?origin=crossref

[100] KREITHEN, MELVIN L. a THOMAS EISNER. Ultraviolet light detection by the homing pigeon. *Nature* [online]. 1978, (vol. 272, 5651), 347-348 [cit. 2019-01-15]. DOI: 10.1038/272347a0. ISSN 0028-0836. Dostupné z: http://www.nature.com/articles/272347a0

[101] Strobe Lights for Bird Control. In: *Pigeon Control Resource Center* [online]. [cit. 2019-01-15]. Dostupné z: https://www.pigeoncontrolresourcecentre.org/html/reviews/strobe-lights-bird-control.html

[102] BLACKWELL, Bradley F., Glen E. BERNHARDT a Richard A. DOLBEER. Lasers as Nonlethal Avian Repellents. *The Journal of Wildlife Management* [online]. 2002, (vol. 66, 1) [cit. 2019-01-15]. DOI: 10.2307/3802891. ISSN 0022541X. Dostupné z: https://www.jstor.org/stable/3802891?origin=crossref

[103] *Phantom 3 Standard Specs* [online]. [cit. 2019-07-25]. Dostupné z: https://www.dji.com/cz/phantom-3-standard/info

[104] Ft - Request use Glonass if GPS is lost and upside down. *DJI Forum* [online]. 22. únor 2018 [cit. 2019-07-12]. Dostupné z: https://forum.dji.com/thread-137189-1-1.html

[105] *DJI Phantom 3 Standard Specs* [online]. Cnet [cit. 2019-07-25]. Dostupné z: https://www.cnet.com/products/dji-phantom-3-standard/specs/

[106] SMITH, Korey. What's the difference between the Phantom 4 and the Phantom 3 Professional?. *MyFirstDrone* [online]. [cit. 2019-07-25]. Dostupné z: https://myfirstdrone.com/blog/differences-phantom-4-phantom-3

[107] Phantom 4 Spec Sheet. *Fullcompass* [online]. [cit. 2019-07-12]. Dostupné z: https://www.fullcompass.com/common/files/27734-DJIPhantom4SpecSheet.pdf

[108] COXWORTH, Ben. DJI introduces simpler, more wallet-friendly Phantom 3 Standard. *New Atlas* [online]. 5. srpen 2015 [cit. 2019-07-25]. Dostupné z: https://newatlas.com/dji-phantom-3-standard-drone/38796/

[109] SULLIVAN, Ben. DJI Is Locking Down Its Drones Against a Growing Army of DIY Hackers. *Motherboard Tech by Vice* [online]. 7. červenec 2017 [cit. 2019-07-12]. Dostupné z: https://www.vice.com/en_us/article/3knkgn/dji-is-locking-down-its-drones-against-a-growing-army-of-diy-hackers

[110] DJI Goggles. *DJI* [online]. [cit. 2019-07-12]. Dostupné z: https://www.dji.com/cz/dji-goggles/info#specs

Seznam obrázků a tabulek