Julie Dahl Hjelle & Line Elisabeth Omli-Moe

Cybersecurity Threats to the Internet of Drones in Critical Infrastructure: An Analysis of Risks and Mitigation Strategies

Master's thesis in Communication Technology and Digital Security
Supervisor: Karin Bernsmed
Co-supervisor: Guillaume Bour

June 2023

Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Julie Dahl Hjelle & Line Elisabeth Omli-Moe

Cybersecurity Threats to the Internet of Drones in Critical Infrastructure: An Analysis of Risks and Mitigation Strategies

Master’s thesis in Communication Technology and Digital Security
Supervisor: Karin Bernsmed
Co-supervisor: Guillaume Bour
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Title: Cybersecurity Threats to the Internet of Drones in Critical Infrastructure: An Analysis of Risks and Mitigation Strategies

Students: Hjelle, Julie Dahl and Omli-Moe, Line Elisabeth

Problem description:

Unmanned Aerial Vehicles (UAVs), commonly known as “drones”, are expected to take over the sky during the next decade. They will deliver packages and medical supplies, inspect and monitor remote areas, and even be used to transport people. In addition, the UAVs will become an integrated part of the controlled airspace, meaning that they (or their pilots) will have to interact with air traffic controllers, just as regular aircraft (and their pilots) do.

The Internet of Drones (IoD) is a relatively new concept emerging from the Internet of Things, replacing “Things” with “Drones”. The IoD is a network architecture that supports coordination of UAVs in the air. IoD can be applied in several application areas, where one of them is critical infrastructure.

With the increasing deployment of UAVs, the security of these devices and the data they collect and transmit are becoming a growing concern. As the IoD continues to expand, the risk of attacks on UAVs is increasing, posing a significant threat to the safety and security of critical infrastructure.

This master’s thesis aims to investigate the current state of security in the IoD, focusing on UAVs used in critical infrastructure and the cyber risks associated with their use. The study will also identify and analyze security mitigations and strategies to reduce the risk of cyber attacks on UAVs. The results of this research will provide valuable insights for organizations that want to use IoD in critical infrastructure, and for those developing security standards for the IoD.

Approved on: 2023-02-24
Main supervisor: Dr. Bernsmed, Karin, NTNU
Co-supervisor: Bour, Guillaume, SINTEF

Abstract

As the deployment of Unmanned Aerial Vehicles (UAVs), commonly known as "drones", is becoming more and more common, ensuring the cybersecurity of these interconnected systems is of huge importance. Internet of Drones (IoD) is a relatively new term arising from Internet of Things (IoT) by replacing "things" with "drones", and hence are prone to attacks just as IoT. Also, as more and more UAVs are connected to the Internet, they can be compromised by an adversary, since everything connected to the Internet is vulnerable. An application area where IoD can be useful, is within critical infrastructure. As such services may have severe consequences if disrupted, it is important that the IoD network is resistant to cyberattacks.

This master's thesis presents a comprehensive analysis of cybersecurity threats to IoD in critical infrastructure. The research aims to identify potential vulnerabilities and effective mitigation strategies to enhance the security of IoD networks. To that aim, we first conducted seven interviews with key stakeholders in the drone sector, including drone operators, communication technology professionals, and industry experts. The interviews provided valuable insights into current practices, challenges, and perceptions regarding cybersecurity threats to UAVs and the IoD. We further conducted a technical experiment with several scenarios focusing on Global Positioning System (GPS) spoofing of the UAVs. The experiment helped us identify the level of difficulty for exploiting the UAVs. Furthermore, we estimated the costs and resources associated with GPS spoofing and Denial of Service (DoS) attacks by using an analysis tool called Resource Cost Model (RCM). The RCM illustrates which steps need to be taken by an attacker to carry out the attacks and gives an indication of how costly the attacks will be. Throughout the semester, we conducted a literature study on existing studies and relevant academic papers on the topic.

By addressing the identified vulnerabilities and implementing several of the proposed mitigation strategies, stakeholders can enhance the security of their IoD networks, especially in critical infrastructure, and thereby ensuring the safe and reliable operation of these systems.

Sammendrag

I takt med at bruken av ubemannede luftfartøy (UAV-er), vanligvis kjent som “droner”, blir stadig mer vanlig, er det av enorm betydning å sikre cybersikkerheten til disse sammenkoblede systemene. Internet of Drones (IoD) er et relativt nytt begrep som oppstod fra Internet of Things (IoT) ved å erstatte “ting” med “droner”, og er dermed utsatt for angrep på samme måte som IoT. Ettersom stadig flere UAV-er er koblet til internett, kan de bli kompromittert av en angriper, ettersom alt som er koblet til internett er sårbart. Et bruksområde der IoD kan være nyttig er innen kritisk infrastruktur. Slike tjenester kan få alvorlige konsekvenser hvis de avbrytes eller forstyrres. Derfor er det viktig at IoD-nettverket er motstandsdyktig mot cyberangrep.

Denne masteroppgaven presenterer en omfattende analyse av cybertrusler mot IoD i kritisk infrastruktur. Forskningen har som mål å identifisere potensielle sårbarheter og effektive strategier og mottiltak for å styrke sikkerheten til IoD-nettverkene. Med dette i bakhodet gjennomførte vi først syv intervjuer med sentrale aktører i dronebransjen, inkludert droneoperatører, kommunikasjonsteknologieksperter og bransjeeksperter. Intervjuene ga verdifull innsikt i nåværende praksis, utfordringer og oppfatninger om cybertrusler mot UAV-er og IoD. Vi gjennomførte også et teknisk eksperiment med flere scenarioer som fokuserte på forfalskning av GPS signalene til UAV-ene. Eksperimentet hjalp oss å identifisere vanskelighetsgraden forbundet med å kompromittere UAV-ene. Videre estimerte vi kostnadene og ressursene forbundet med GPS-forfalskning og Denial of Service-angrep ved hjelp av et analyseverktøy som kalles Resource Cost Model (RCM). RCM viser hvilke steg en angriper må ta for å gjennomføre angrepene, og gir en indikasjon på hvor kostbare angrepene vil være. I løpet av semesteret gjennomførte vi også en litteraturstudie om eksisterende studier og relevante vitenskapelige artikler om emnet.

Ved å adressere de identifiserte sårbarhetene og implementere flere av de foreslåtte strategiene for risikoredusering, kan operatører av kritisk infrastruktur styrke sikkerheten til sine IoD-nettverk og dermed sikre en trygg og pålitelig drift av disse systemene.

Preface

This master's thesis was written as the final part of our 5-year Master of Science Degree in Communication Technology and Digital Security, with the Information Security specialization at the Norwegian University of Science and Technology (NTNU). The thesis was written during the spring of 2023 in cooperation with SINTEF and builds upon the authors' pre-project that was carried out in the fall of 2022.

We want to thank our supervisors, Karin Bernsmed and Guillaume Bour, for continuous feedback and guidance throughout this semester. Guillaume helped us get in contact with several participants for our interviews and provided suggestions and help during the experimental part.

We also want to express gratitude to the interviewees that agreed to take part in our research.

Contents

Appendices

List of Figures

List of Tables

List of Acronyms

ADS-B Automatic Dependent Surveillance-Broadcast.

ARP Address Resolution Protocol.

ATC Air Traffic Control.

ATF Air Traffic Flows.

ATM Air Traffic Management.

AUV Autonomous Underwater Vehicle.

BLoS Beyond Line-of-Sight.

CAGR Compound Annual Growth Rate.

CIA Confidentiality, Integrity and Availability.

CISA Cybersecurity & Infrastructure Security Agency.

CKC Cyber Kill Chain.

DDoS Distributed Denial of Service.

DoS Denial of Service.

EASA European Aviation Safety Agency.

ECC Elliptic Cruve Cryptography.

FAA Federal Aviation Administration.

GCS Ground Control Station.

GGACS-IoD Generic Access Control Scheme for the Internet of Drones.

GNSS Global Navigation Satellite System.

GPS Global Positioning System.

GSS Ground Station Server.

ICAO International Civil Aviation Organization.

IDS Intrusion Detection System.

IoD Internet of Drones.

IoT Internet of Things.

ISM Industrial, Scientific and Medical.

ITU International Telecommunication Union.

LiDAR Light Detection and Ranging.

LOIC Low Orbit Ion Cannon.

LoS Line-of-Sight.

MAC Medium Access Control.

MEC Mobile Edge Computing.

MITM Man-in-the-Middle.

NATO North Atlantic Treaty Organization.

NGAD Next Generation Air Dominance.

NTNU Norwegian University of Science and Technology.

RADAR Radio Detection and Ranging.

RCM Resource Cost Model.

RF Radio Frequency.

RNN Recurrent Neural Networks.

RVI Remote Visual Inspection.

SATCOM Satellite Communication.

SDR Software Defined Radio.

SITL Software in the Loop.

TCALAS Temporal Credential-Based Anonymous Lightweight Authentication Scheme.

ToF Time of Flight.

UAV Unmanned Aerial Vehicle.

USV Unmanned Surface Vehicle.

UTM Unmanned Traffic Management.

VLoS Visual Line-of-Sight.

Chapter 1 Introduction

1.1 Motivation

Unmanned Aerial Vehicles (UAVs) is the technical name for “drones”. They are aircraft that do not have a pilot on board. Instead, they can be configured to fly autonomously or be remotely controlled by a pilot. UAVs are becoming a bigger part of our lives. They are useful for a diversity of tasks, among them inspections, search and rescue operations, delivering packets, and many more. As the production costs of microprocessors and other hardware parts used for UAVs have decreased significantly in recent years, they have become affordable and common goods. [KL22]

UAVs take part in the digital transformation or the digital shift, where most parts of society and businesses are influenced by technology. However, with digitalization come digital risks, and the number of cyberattacks has increased rapidly over the last few years. UAVs are no exception and are indeed vulnerable to such attacks.

With the use of different sensors, UAVs can gather vital information. Because of the value of this information, adversaries may try to gain access to it in order to sell it or use it themselves. In some cases, the outcome can be devastating or have severe consequences if such information gets into the wrong hands [YWY+22][MRV22]. Unauthorized control of a UAV can in the worst scenarios have a fatal outcome. This highlights the importance of a robust and secure UAV system, that should resist cyberattacks [YWY+22]. Unfortunately, there have been several exploits of UAVs. Some examples are discussed in Section 3.5.

The Internet of Drones (IoD) provides coordinated access to controlled airspace for the UAVs [GBW16]. It is a network of UAVs that can exchange information [CSG+18]. IoD has become a popular topic because of its advantages like portability, automation, and mobility [YWY+22], and its many application areas. An interesting application area of IoD is within critical infrastructure. Many industries are already using UAVs to monitor and inspect their industrial sites. With the use of IoD, the data gathering can be more efficient, and operators can get real-time data from different places.

Not surprisingly, IoD is also subject to cyberattacks and can be used to harm critical infrastructure. State actors and others that wish to gather intelligence on other countries' operations, or disrupt them, can attack the IoD network used in critical infrastructure. They can either attack the UAVs by, for example, hijacking them or sending spoofed signals to make them crash in the installations. Moreover, they can deploy a malicious UAV to inspect the infrastructure. This is explained further in Chapter 3.

1.2 Objectives and Research Questions

UAVs are susceptible to several cyberattacks, and this thesis aims to identify the possible risks and vulnerabilities in a UAV system. As IoD is rapidly evolving and can provide valuable services for operators of critical infrastructure in the future, we will look at how both UAVs and IoD are affected by cyberattacks, and what measures can be done to handle the threats and mitigate the risks they are facing. We will also address the level of difficulty to perform such attacks from a technical perspective, as well as a resource and cost perspective.

To achieve this, we aim to answer the following research questions that are maintained from our pre-project [OH22]:

RQ1 What are the security risks when it comes to the use of IoD within critical infrastructure?

RQ2 How difficult would it be to exploit the UAVs both technically and from a resource and cost perspective?

RQ3 What mitigations can be applied to the IoD to overcome these risks?

1.3 Structure of the Thesis

Chapter 1 includes our motivation, objectives, and research questions. Chapter 2 presents the different methods that will be used to answer the research questions. Relevant background material and related work are introduced in Chapter 3. Our results are presented in four chapters, each providing a different perspective that answers one or more of the research questions. The findings from our interviews are presented in Chapter 4. Chapter 5 includes a description of what software was evaluated and eventually used for the experiments. It also explains the approach of the experiments and presents the results. Chapter 6 provides a resource and cost analysis of two chosen cyberattacks. Chapter 7 is also a part of the results, and it summarizes the cyber threats found in the literature studies and interviews. It has visual representations of some of the cyber threats and a table summarizing them. The results are discussed in Chapter 8, and the conclusion and future work is presented in Chapter 9. The interview guide and relevant scripts are attached in Appendix A, B, and C.

1.4 Scope

In this thesis, our focus was not on the communication algorithms for UAVs in IoD. Instead, we wanted to see how difficult it would be to exploit a UAV. Also, due to safety and feasibility, the experiments were performed on simulated UAVs instead of real ones. Moreover, in this thesis, our emphasis was primarily on threats rather than risks. Therefore, the assessment of likelihood and consequences has not been taken into account.

Chapter 2
Methodology

To address the research questions presented in the introduction, four different methodologies were used; a literature review, interviews, technical experiments, and modeling resource costs. The methodologies enable the readers to assess the validity and reliability of the conducted research. This chapter highlights the relevance these methods have for the topic, and that they can provide some contribution to our research. The methodologies are elaborated on and justified further below, and they were carried out in that order. Figure 2.1 presents a visual representation of the methodologies used to answer which research question(s).

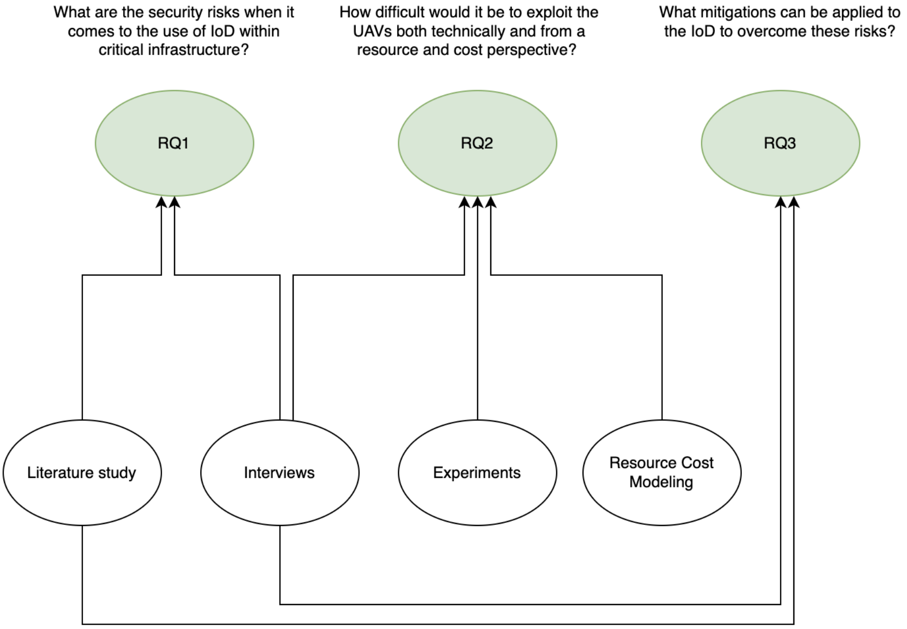

What are the security risks when it comes to the use of IoD within critical infrastructure?
How difficult would it be to exploit the UAVs both technically and from a resource and cost perspective?
What mitigations can be applied to the IoD to overcome these risks?
RQ1
RQ2
RQ3
Literature study
Interviews
Experiments
Resource Cost Modeling

Figure 2.1: Methodology model

2.1 Literature Review

As a foundation, this thesis is based on literature studies. This provided a broader understanding of the topic and it included finding existing work done by others. As mentioned in our pre-project [OH22], we relied on academic sources i.e. Engineering Village,[1] IEEE Digital Library,[2] Scopus,[3] ACM Digital Library,[4] and Springer[5] to find papers. These sources provided a variety of research articles. Relevant keywords used when searching for articles included *UAV, IoD, vulnerabilities, swarm, critical infrastructure, drones, privacy, security* and *mitigations*, but were not limited to these only. An analysis of the literature findings is presented in Chapter 7.

2.2 Interviews

For this thesis, seven interviews were conducted. The interviews allowed us to gather new, in-depth information on the topic we can contribute with, and to get a better understanding of UAVs and IoD from people with knowledge about this. The interviewees were people relevant within the drone sector. They could have been either working with or doing research on drones, drone security, communication technology, or the IoD. With respect to privacy, we will not go into further details about them. Some of the interviewees were selected by obtaining their contact information from our co-supervisor, and others by finding relevant companies or organizations and looking up contact information online. They were primarily contacted via e-mail.

The interviews were held in a semi-structured way, which implied open-ended questions with follow-ups [DV19]. It was more similar to a dialogue between the interviewer and the interviewee rather than short yes-no replies. We alternated on who held the interviews and who took notes. A general interview guide was made, and it was modified to fit each participant in the best way. We first introduced ourselves and presented our project in a short manner. Then, we asked about what they worked with, and for how long, to get insight into who we were talking to and what competence they might have. With the interview guide, we wanted to find out how the interviewees used UAVs or IoD today, what mitigations they had for cyber threats, and what they knew about IoD and UAVs in critical infrastructure. Furthermore, it was useful to get their opinion on benefits, limitations, and future outlooks regarding UAVs and IoD. After each interview, we learned to improve the questions to ask the following participant and were able to improve the interview guide.

[1] https://www.engineeringvillage.com/

[2] http://ieeexplore.ieee.org/

[3] http://www.scopus.com/

[4] https://dl.acm.org/

[5] https://link.springer.com/

All seven interviews were held digitally using Microsoft Teams,[6] Gooogle Meet,[7] or Signal.[8] Microsoft Teams is a video conference tool provided by Microsoft, and Google Meet is a similar application developed by Google. Signal is a messaging application that provides end-to-end encryption using the open-source Signal protocol. This was required to use by some of our interviewees, as secure communication and privacy were important to them. All three applications provide chats and video calls. The interviews were held in either English or Norwegian, depending on who we were talking to.

The interviewees gave us written consent prior to their interview for us to do a sound recording during the interview, to ensure that no important information was missed. The mp4-file was transcribed using the OpenAI's Whisper[9] tool. It is a Python package that was installed locally on our computers using Pip.[10] Whisper ran locally without calling an API, preserving data privacy. The generated text was thoroughly checked and inconsistencies were fixed.

Further, the transcription of the interviews was anonymized and uploaded to Nvivo.[11] This software helped us organize, analyze and find patterns and insights in our qualitative data. Nvivo was an installed program on our computers.

2.3 Experiments

A few experiments were performed where the aim was to get an understanding of the complexity and the level of difficulty to exploit vulnerabilities present in UAVs and compromise them.

To perform the experiments, we decided a simulator was suitable. A reason why we did not use a real UAV was the lack of UAVs to test on, as well as safety. As our thesis is about IoD, we aimed to find a simulator that allowed the creation of multiple UAVs, to observe the impact in an environment where there were more than one UAV. Possible scenarios were to simulate one or multiple UAVs that flew autonomously or were controlled by a Ground Control Station (GCS). The attack chosen to be performed was GPS spoofing. For these purposes, many open-source tools and simulators were evaluated to find their limitations and figure out if they fitted our scenario. The attack setup and results are described in Chapter 5.

[6] https://www.microsoft.com/nb-no/microsoft-teams/group-chat-software

[7] https://meet.google.com/

[8] https://signal.org/

[9] https://openai.com/research/whisper

[10] https://pypi.org/project/pip/

[11] https://i.ntnu.no/wiki/-/wiki/English/NVivo

2.4 Resource Cost Modeling

It is important to understand the costs, benefits, and attractiveness of cyberattacks to understand how to prevent them. This can be done by utilizing the Resource Cost Model (RCM) developed by Haga [Hag20]. The model associates each stage of a cyberattack to a resource cost, and hence you can find the total cost of performing such an attack. To define the stages of a cyberattack, the RCM utilizes a kill chain, and couples each stage with a resource tree. The structure of the model is illustrated in Figure 2.2. [Hag20]

2.4.1 The Cyber Kill Chain

The Cyber Kill Chain (CKC) is a way of identifying and preventing cyber intrusions activity by describing each stage of a cyberattack [Mar22b]. There are several variants of this method, and the number of stages can vary. This thesis will use the method formulated by the American aerospace and security company Lockheed Martin.[12] They aim to provide secure and cyber resilient systems across their products [Mar22a]. The CKC is one of their tools for intelligence-driven computer network defense, and it consists of seven stages an attacker must complete successfully in order to accomplish his objective. This framework is useful to get insight and awareness of the attacker's tactics, techniques used, and procedures followed [Mar22b]. Only one mitigation technique is needed to break the chain and prevent an attacker from proceeding toward his goal. The CKC is widely used among IT companies and enterprise networks [HCA11]. The stages are as follows: [HCA11][Hag20][Mar15]

1. **Reconnaissance -** Identify the targets

   A planning phase where adversaries select their target by understanding which targets can help them meet their goals. They gather e-mail addresses, identify employees on social media, and collect press releases and conference attending lists.

2. **Weaponization -** Prepare the operation

   A "weaponizer" is used for coupling malware and exploits it into a deliverable payload like a PDF, Microsoft Office document, or an image. This will act as a weapon.

3. **Delivery -** Launch the operation

   Transportation of the weapon to the intended environment. This is usually done by an e-mail attachment, website, or flash drive.

[12] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

4. **Exploitation** - Gain access to the victim

   The malicious code is triggered on the victim's system by exploiting a vulnerability in an application or an operating system, or it is triggered unknowingly by the user itself.

5. **Installation** - Establish a foothold at the victim

   Installation of the malware on the victim system. Usually, a backdoor is used to have persistent access to the environment.

6. **Command & Control** - Remotely control the implants

   Establishment of a channel for the intruder to have access to the target environment.

7. **Actions on Objectives** - Achieve the mission's goal

   The intruders can now take actions to complete their objectives. Often, they aim to extract data, encrypt information or violate integrity or availability.

2.4.2 Resource Trees

Attack trees were first defined in 1999 by Bruce Schneier, then CTO of Counterpane Internet Security. It is a method for modeling security threats. The reasons for needing a method for this are to get an understanding of who the attackers are and what goals they have, what attacks are likely to occur, and where to best spend a security budget. The trees are helpful to visualize attacks and the possible countermeasures, where the root node of the tree is the objective [Sch99]. Schneier [Sch99] also showed that a cost or time perspective can be allocated to the nodes in the tree. Resource trees are inspired by these attack trees.

As mentioned above, in the RCM each CKC stage has a corresponding resource tree, which derives the cost of all required resources at the designated stage. The resource trees have three levels: kill chain stage, resource, and resource alternative. The latter are the leaf nodes and present the alternatives an attacker has when it comes to obtaining the resource in the level above. There can be several resource alternatives, hence an attacker only needs to get hold of *one* to realize its parent resource [Hag20]. This is noted by "OR" in the trees. The resources are categorized into the following five: [HMS20][Hag20]

- ◇ **Skill** - domain knowledge like programming skills or knowing how to use certain cybercrime tools.
- ◇ **Behavioral** - includes actions that have to be completed in order to carry out the attack, e.g. connecting a flash drive, bribing, or a victim opening a phishing-mail.

- ◇ **Tangible -** physical resources e.g. a computer or a signal jammer.
- ◇ **Logic -** commercially available software, data sets or cybercrime tools. Github repositories or Remote Access Trojans are in this category.
- ◇ **Logic-atomic -** resources that cannot be further divided, like IP addresses or passwords.

The kill chain stage level, i.e., the root node, is either of the seven stages in the CKC, and the attacker has to get hold of *all* resources needed in each stage to proceed to the next stage. This is noted by “AND” in the trees. [Hag20]

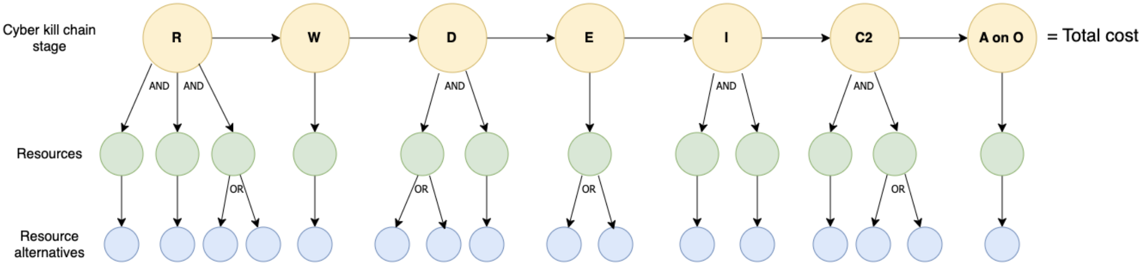


Figure 2.2: Resource cost model (inspiration from [Hag20])

2.4.3 Estimating Monetary Cost

For an attack to be successful, all the seven stages of the CKC need to be completed. Hence, the total cost of an attack is the sum of the costs associated with each stage. The cost varies, and factors influencing the cost are which resource alternatives are chosen to realize the resources. Each resource alternative has an associated minimum to maximum cost and a confidence value. A confidence value in proximity to zero indicates that there is little evidence supporting the defined cost interval. On the other hand, a value close to 1 indicates grounds to say that the cost interval is not varying much. [Hag20]

The estimated cost interval of an attack is the sum of the minimum and the sum of the maximum cost estimates for each stage. The confidence for each stage is the product of the average confidence values of the resource alternatives needed to realize each resource. Total confidence is the product of the confidence values calculated for each stage. In the equations below, the cost of the cheapest and most expensive resource alternatives are represented with α and β respectively. V is a set of resource alternatives for the attack stage. ϕ defines the average confidence value of the n

resource alternatives for a resource. [Hag20]
This gives: [Hag20]

$$Estimated\ cost = [Min\_cost, Max\_cost, Confidence] \tag{2.1}$$

$$Min\_cost = \sum_{stage \in CKC} \sum_{i \in V} \alpha_i \tag{2.2}$$

$$Max\_cost = \sum_{stage \in CKC} \sum_{i \in V} \beta_i \tag{2.3}$$

$$\phi_j = (\sum_{i \in R_j} c_j)/n \tag{2.4}$$

$$Confidence = \prod_{stage \in CKC} \prod_{j \in R} \theta_j \tag{2.5}$$

2.4.4 Why Resource Cost Modeling is Suited for the Thesis

The second part of **RQ2** is to figure out how difficult it is to exploit the UAVs from a resource and cost perspective. The RCM can provide an understanding of how difficult this would be by estimating the resources required and the total cost. As both the minimum cost and the maximum cost is estimated, it can help us get an idea of who are able to accomplish such attacks. This makes the RCM a good choice for this thesis.

2.5 Ethics and Privacy Concerns

We applied to NSD[13] because we wanted to do sound recordings during the interviews. We got approval before the interviews took place, and we also got written consent from each interviewee. During the interviews, the interviewees were asked once again if they consented to a sound recording. If yes, the recording was started, and the question was repeated to get consent on tape.

Personal information from the interviews was anonymized and processed locally on our computers. The sound recordings and transcriptions of the interviews were deleted at the end of the project.

[13] https://www.nsd.no/index.html

Chapter 3 Background and Related Work

Identification of relevant background material and related work was carried out in the project preceding this thesis [OH22]. New literature studies have been conducted to gather more relevant information and added to complement the material previously gathered. This chapter includes information about UAVs, IoD, and cybersecurity aspects like threats and proposed mitigation techniques. During the research, some papers also included examples of attacks that had happened more recently. Those are included as well. Relevant research from the preceding project has been cited.

3.1 Unmanned Aerial Vehicles

3.1.1 Types

UAVs exist in different variants, and the sizes can vary from the size of an insect to the size of a commercial airplane. The most common UAVs are either multi-rotor systems or fixed-wing systems, and the majority of UAVs can be categorized into these two. There also exist UAVs that have characteristics of both types, but these are less frequent. [VNBC16]

Multi-Rotor

A multi-rotor can have up to eight rotors on the platform, but the most popular is the quadcopter with four rotors. The quadcopter is also called a helicopter and exists in both big and small ones in different price ranges. The smaller models are common in the hobby market, but re-built models are also used in the war in Ukraine [Pol23]. The top three commercial vendors for quadcopters in 2023 are the Chinese DJI,[1] and Yuneec[2], and American Parrot[3] [Coa23]. Multi-rotor UAVs are often used for

[1] Da-Jiang Innovations, https://www.dji.com/no

[2] https://yuneec.online/

[3] https://www.parrot.com/us/drones

photography or filming from the air. Bigger ones can be used for transport and search and rescue operations [Pol23]. [OH22]

Fixed-Wing

Fixed-wing UAVs are similar to aircraft and require a runway for takeoff, or they can use a catapult launcher. These UAVs are usually bigger and can have a wingspan of up to several meters. They are more expensive and demanding to operate than quadcopters, so state actors or organizations with a lot of funds are usually the ones using this type of UAVs [Pol23]. UAVs with fixed wings often are used for measuring, mapping, or monitoring larger geographical areas. An example of a fixed-wing UAV is Raven.[4] There also exist hybrid UAVs, which have fixed wings but still are able to take off and land vertically [Luf22]. [OH22]

Miniature UAV for Reconnaissance

Single rotor UAVs, while more efficient, are less common. This is mostly due to their higher mechanical complexity and maintenance cost. The Black Hornet PRS[5] is an example of a single rotor UAV [OH22]. The Black Hornet 3 is a Norwegian-developed UAV that can fly in bad weather conditions and can handle extreme cold and heat. The UAV is used by the defense, police, and national security organizations in over 40 countries. The Black Hornet costs around 2 million NOK per UAV, which is approximately $190 000 [Pol23].

3.1.2 Regulations

A common European regulation exists for UAVs in the EU and Norway [Lufa]. In Norway, all UAV operators must register at www.flydrone.no, and the registration fee is 220 NOK, which is almost $20 [Lufb]. The new regulations require new UAVs on the market today to have a C-classification mark from C0 to C4, where different regulations relate to different marks [Luf22]. There are some areas where a UAV operator is not allowed to fly, and it is important to be aware of such areas. The no-fly zones include areas close to airports, and it is not allowed to fly closer than 5 km to an airport without permission from the Air Traffic Control (ATC) [Lufa]. There are also restricted areas where you need permission to fly, for example in cities. Forbidden areas include military areas, prisons, natural parks, and embassies. [OH22]

Ninox Drone is an application that can be downloaded on smartphones where operators can request access to controlled airspace, view airspace restrictions, receive messages from air traffic controllers, and access other relevant information [AS20]. In the future, there is some automation planned for the Unmanned Traffic Management

[4] https://www.avinc.com/uas/raven

[5] https://www.flir.eu/products/black-hornet-prs/

(UTM) where the UAVs operate. The full integration between manned and unmanned airspace is planned to take place in 2025-2035 [Knu].

In April 2021, a regulation on U-space was adopted. From a common European point of view, there has been an urgent need to establish some common frameworks on how air traffic services for UAVs are to be regulated. The regulation took effect on the 26th of January 2023. U-space could be described as a comprehensive solution for how UAVs can operate simultaneously in low airspace, especially in densely built-up areas, in a safe, efficient, and secure way. U-space will show how UAVs will integrate with manned aviation [Reg17].

3.1.3 Technical Aspects

In our pre-project [OH22] we created an illustration of a high-level architecture of a UAV system, which can be seen in Figure 3.1. The UAV system consists of a GCS and a UAV. The communication between the entities happens directly over a data link or via a network/satellite. The UAV has aircraft hardware which is the frame, motors, rotors, and the physical components of the system. There is also a component for onboard computing that does the logic. Actuators and sensors in the UAV include different IoT smart sensors [BCD20]. Some of them are GPS, light-pulse distance sensors (laser), Radio Detection and Ranging (RADAR) sensors, sonar-pulse distance sensors (ultrasonic), and Time of Flight (ToF) sensors.

To operate, the UAV needs an energy supply. This could be battery cells, solar cells, and traditional airplane fuel [VNBC16]. UAVs can have a payload on board. The various types of payload can for instance be mail parcels or medicines for transportation, fire extinguishers, or flyers. It can also be cameras, sniffers, and meteorological sensors [VNBC16]. What payload the UAV has depends on what weight it can carry and the intended use cases.

For communication, the UAV has the option for wireless technologies, like for instance WiFi, satellite, mobile networks, and/or ADS-B. The communication can either be direct, Line-of-Sight (LoS) communication, or indirect with Satellite Communication (SATCOM) [HS13]. Indirect communication is called Beyond Line-of-Sight (BLoS), and the UAV is no longer visible to the GCS. Visual Line-of-Sight (VLoS) means the remote pilot can see the UAV clearly [OH22]. These concepts are illustrated in Figure 3.2.

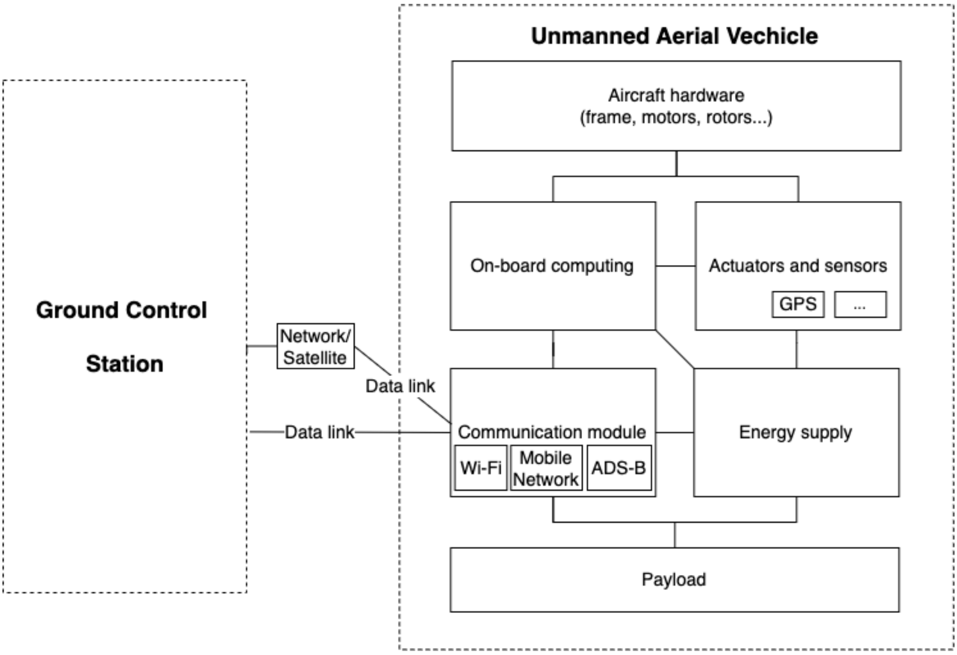


Figure 3.1: High-level architecture of a UAV system (from [OH22])

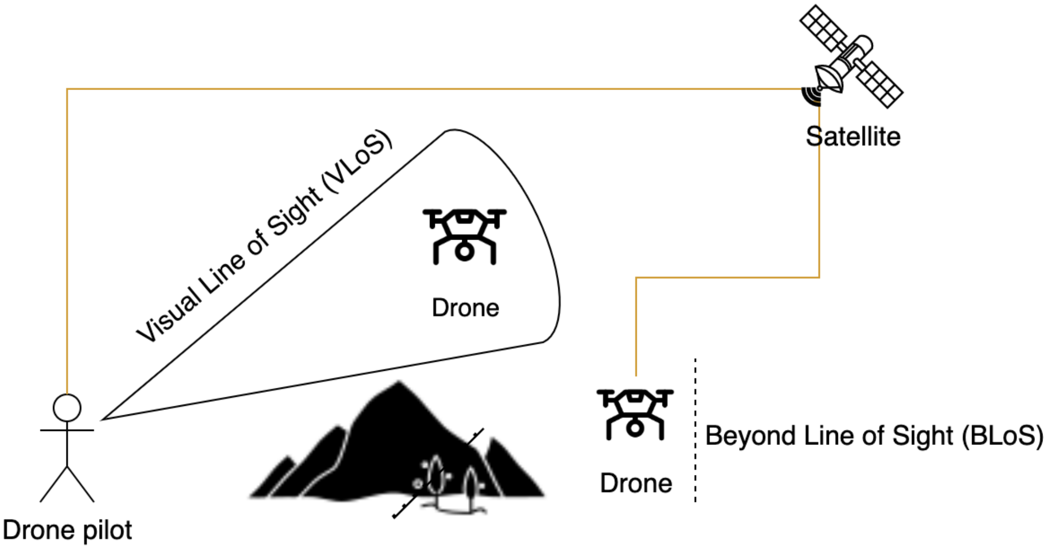


Figure 3.2: VLoS and BLoS (from [OH22])

In LoS communication, the C-band or WiFi are often used for transmissions. The C-band includes the electromagnetic spectrum ranging from 4 GHz to 8 GHz [HS13]. The specific communication depends on the UAV type. In WiFi, the frequencies and transmission rates depend on the chosen standard. For the latest DJI UAVs, Bluetooth is also supported and is used to transfer photos taken by the UAV to the mobile phone via the DJI Fly app. This app is used to provide live videos and additional controls. UAVs use different operating systems, however, most of the DJI UAVs are based on Android. DJI encrypts its firmware with AES and uses RSA to sign it [SCS+22].

The majority of consumer UAVs have a high-resolution camera attached to a gimbal. The function of the gimbal is to compensate for the movement of the UAV and as a result provide a steady image. Some UAVs can also have an extra camera for collision avoidance. UAVs use infrared or ultrasonic sensors to measure the altitude of the UAV, or accelerometers and gyroscopic sensors that measure acceleration and tilt. [SCS+22]

Drone manufacturers introduce measures to ensure safe and secure use of UAVs. For instance, they impose software limitations regarding speed and altitude and use geofencing to create no-fly zones around, for instance, airports and prisons. [SCS+22]

UAVs from the leading drone manufacturer, DJI,[6] implement a tracking protocol called DroneID. The tracking protocol transmits the position of both the UAV and its operator to law enforcement or operators of critical infrastructure [SCS+22]. This allows for the parties to track UAVs and prevent malicious operators. This generation of DJI UAVs use the OcuSync protocol for wireless transmission in the 2.4 GHz and 5 GHz Industrial, Scientific and Medical (ISM) bands [SCS+22]. OcuSync is DJI's transmission protocol and has a range of about 15 km.

Another characteristic of UAVs is the degree of autonomy. The UAV can vary from being fully controlled by a remote pilot to being fully autonomous [VNBC16]. Autonomous UAVs can make their own decisions if something unexpected happens.

From a technical point of view, it is the communication module and the actuators and sensors that send out or receive information, that are prone to attacks. The wireless data link controls the UAV and is accessible remotely so it can be categorized as an important attack vector. [SCS+22]

Automatic Dependent Surveillance-Broadcast (ADS-B) is an Air Traffic Management (ATM) and ATC system used for navigation and localization of other aircraft. As aircraft use ADS-B to broadcast their position, speed, heading, and other data periodically, others nearby will know where they reside and are headed [GBW16][HAR22].

[6] DJI had a market share of 94% in the consumer drone segment in 2021 [SCS+22]

This is an important feature to avoid collisions and optimize air traffic. It is intended to replace the traditional radar-based systems and is expected to be an important part of the next generation of air transport systems [Cos22].

Today, most aircraft are equipped with an ADS-B OUT transmitter. Its role is to broadcast identification information and current positions in periodic intervals to the GCSs or other aircraft over the 1090 MHz band [YMB+19]. According to regulations from European Aviation Safety Agency (EASA) and Federal Aviation Administration (FAA), it was mandatory for all aircraft operating in European and U.S. airspace to have ADS-B capabilities by 2020. If the regulation applies to the UAV depends on factors like how big it is, the type, how far and high it will fly, and what airspace rules apply [Gro21][OH22]. ADS-B lacks the basic security mechanisms like encryption and authentication, making it vulnerable to attacks [YMB+19].

ADS-B IN is a technology mainly used in ATC towers or the GCS. It is a transceiver that receives the signals from the OUT device. Some challenges related to ADS-B IN are verifying the identity of the aircraft and real-time validation of the location data, as the connection to the aircraft differs. [Cos22] Due to these challenges, the ADS-B IN system can sometimes display a "ghost plane", but in theory, this should not happen with aircraft equipped with ADS-B OUT. What happens is that the ATC towers cannot correlate between the radar target and the position received directly from the ADS-B OUT transmissions. The towers will not risk missing reporting a conflict, so they rebroadcast the radar data as an anonymous target, unintentionally displaying a "ghost plane" on the screen [Sok16].

3.2 The Internet of Drones

UAVs are becoming smaller, lighter, more efficient, and cheaper. In addition to becoming more autonomous in the future, UAVs will also be able to operate in swarms [VNBC16]. IoD is a further extension from IoT, where "things" are replaced with "drones" [MRV22]. The properties and characteristics of the IoD are similar to the IoT. While IoT devices are typically static, drones, or UAVs, are mobile. IoD facilitates UAV cooperation and allows them to join and form a network, which enables the exchange of data between them. IoD plays an important role in the development and future of UAVs [REAE21].

Figure 3.3 presents three existing IoD architectures: IoD architecture based on cloud, IoT-based IoD architecture and the Internet-based IoD architecture [MRV22].

The cloud-based IoD architecture enables virtualization access to UAVs over the cloud and the ability to upload substantial computations to the cloud environment using minimal resources. The architecture has three levels which include the drone layer, the cloud layer, and the client layer. The drone layer is the first layer and it represents a collection of resources/services that will be made available to end consumers. The second layer is the cloud layer which contains storage components for storing a stream of data generated by UAVs, processing components, and an interface component. The third and last layer is called the client layer, which has interactions with the other two layers. [MRV22]

The IoT-based IoD architecture takes into account the different IoT sensors that can be present on UAVs. The architecture has connections between the UAVs in the flying zone, between the UAVs and the Ground Station Server (GSS), and between the GSS and the control room. [MRV22]

The Internet-based IoD architecture has five entities. These are UAV flying zones, a centralized server that oversees all IoD tasks, a control room, an Internet-based channel, and users [YIA+21]. The server is considered the trusted entity in this architecture, so an assumption is that it will not be compromised by an attacker [WDL18].

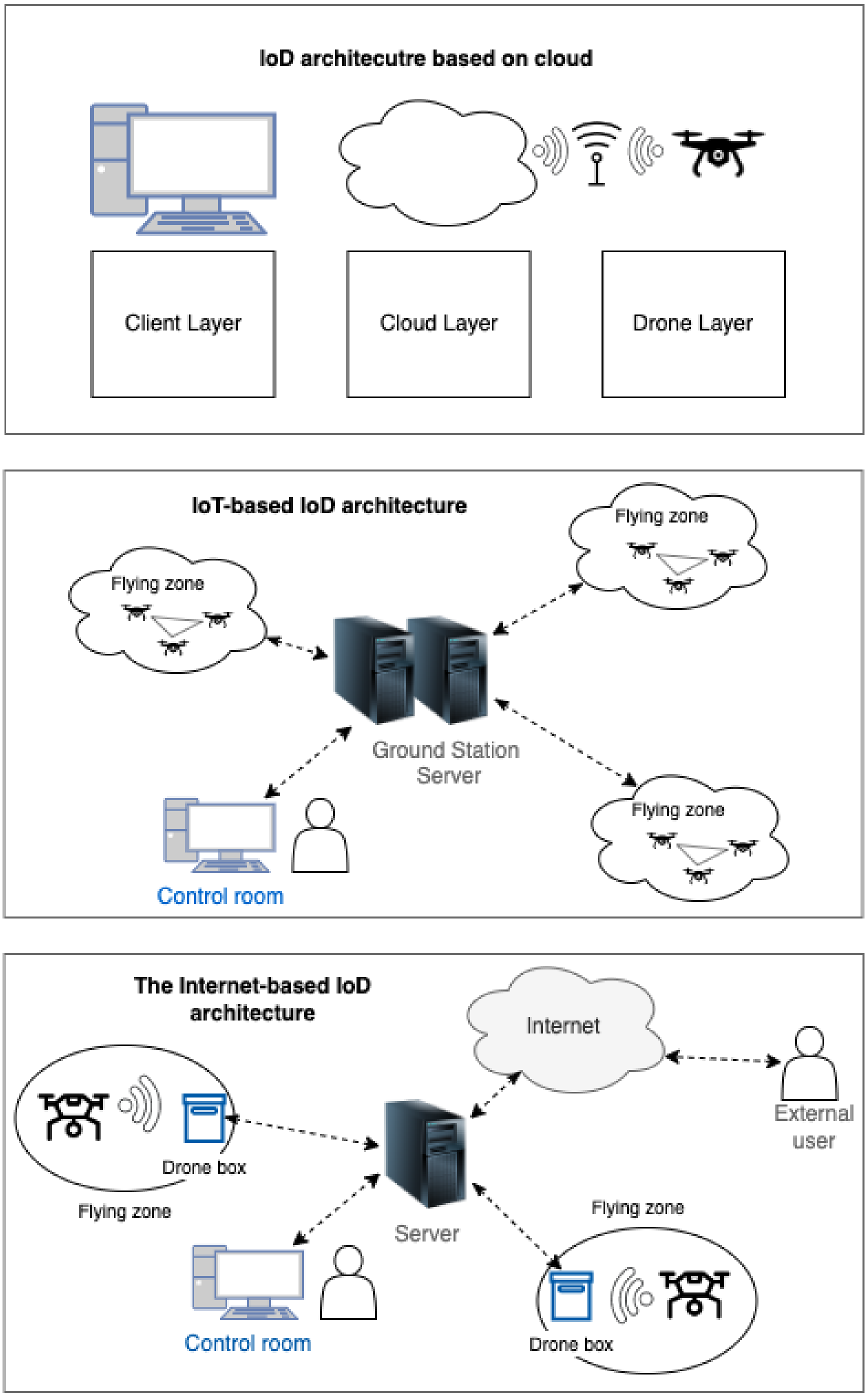


Figure 3.3: IoD architecture types (adapted from [MRV22][OH22])

3.2.1 Applications

UAVs can offer advantages and opportunities in many different applications. These applications include agriculture, military, delivery, healthcare, and medical services [YWY+22]. Some application areas are summarized in Figure 3.4.

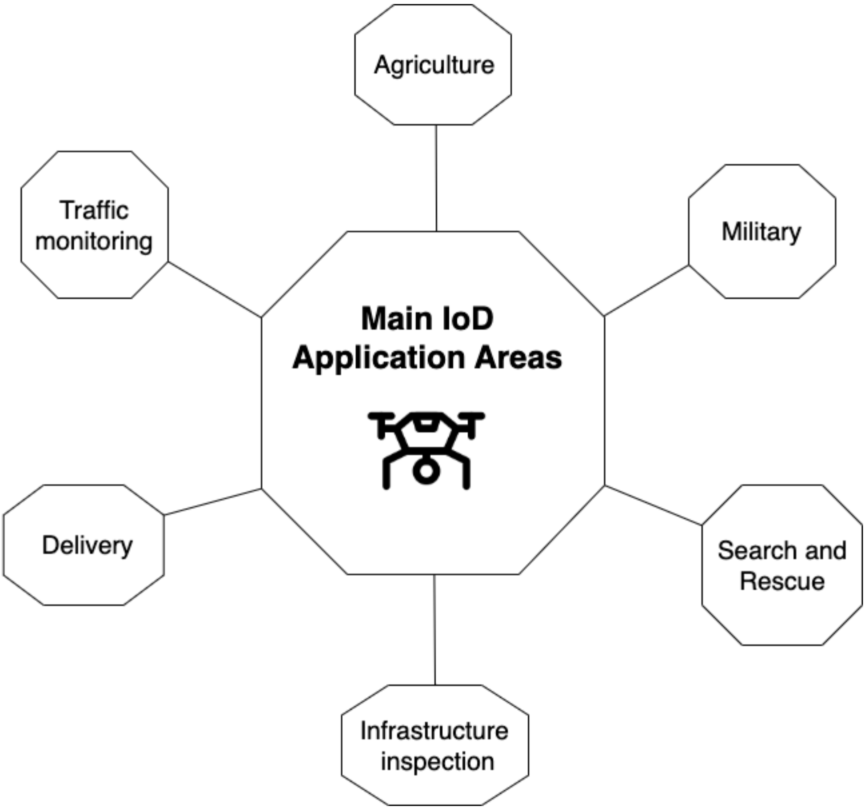


Figure 3.4: IoD Application Areas (adapted from [YWY+22])

Military

Historically, UAVs were made for warfare and military use. They are increasingly applied in modern conflicts [Gar21], and in more recent days, we have seen that UAVs are used in the conflict between Russia and Ukraine. UAV use for military purposes has become a significant IoD application [YWY+22]. When flying with a pilot on board seems to be too dangerous or challenging, i.e. using a helicopter or an airplane, a UAV can be used. Military UAVs are suitable in missions concerning reconnaissance, surveillance, assisting in selecting targets for military attacks, and can also help with combat tasks [YWY+22].

While there is an increased use of UAVs for military purposes, this does not mean that they will replace manned aircraft just yet, but we will see a time where both will collaborate. As an example, the next generation of some American fighter jets will be able to cooperate with UAVs. The new manned 6th-Generation stealth fighter jet planes will have the ability to operate up to five UAVs from the cockpit. The US Air Force may build several manned variants of the 6th-Generation Next Generation Air Dominance (NGAD) stealth fighter jet and a collection of wingman-type support UAVs. [Osb23]

Agriculture

For use within agriculture, UAVs can help farmers obtain information about the soil and the plants, so the farmer can make the best decisions. By using IoD, farmers can get early warnings about threats so they are able to neutralize them at the earliest stage. Benefits of UAVs in agriculture include agricultural farm analysis and improvement in agricultural yields [YWY+22]. UAVs can take photos and do analysis through geographic indicators to find out where there exist infected areas so pesticides can be sprayed. IoD do this safer and more efficiently than humans. In Japan, 30% of rice fields are being sprayed with UAVs [VNBC16].

Search and Rescue

Natural disasters are occurring more frequently as climate change is getting worse. Because of this, search and rescue operations are very important today. UAVs used in IoD are powerful tools for search and rescue operations because of the available sensors and cameras [YWY+22]. UAVs can help find the location of lost or injured humans, especially in difficult terrain.

Infrastructure Inspection

UAVs can be applied as inspection tools to a wide range of businesses. Critical infrastructure, including healthcare and aviation, are some potential domains for UAVs. UAVs in critical infrastructure is further elaborated below in Section 3.4.2.

Delivery

UAVs can be used for transportation of medical supplies, like vaccines, blood bags, and medicines, to remote developing countries during health emergencies [YWY+22]. Effective medical deliveries done by UAVs may save lives. Zipline[7] is an American drone delivery company that specializes in automated delivery. Currently, they have head responsibility for blood bag delivery in Rwanda, and during the Covid-19 pandemic, they distributed vaccines in Ghana. They also deliver other goods like

[7] https://www.flyzipline.com/

takeaway food and groceries [Zip]. Aviant[8] provides similar services as Zipline, only in some parts of Norway and Sweden. UAVs can also be used to deliver packets. Big corporations like Amazon, Google, and Facebook have started to deliver products with UAVs in addition to humans [SDKR19].

Traffic Monitoring

UAVs can be used to collect data about traffic that can further be used to investigate congestion issues [YWY+22]. Using IoD for this purpose can produce a comprehensive data set for traffic areas. In case of traffic jams, it is possible to reroute the traffic [VNBC16]. Researchers have designed an IoD system that can be used for traffic speed monitoring [YWY+22].

There are also other applications like smart cities, entertainment, logistics, automation, tracking, and wildlife research [YWY+22]. The future of IoD can have an impact in many areas.

3.3 Cybersecurity

Cybersecurity is very important nowadays, as more aspects of our lives are digital, and the use of the Internet is growing rapidly. There are many risks related to digitalization, and if poor security configurations are in place, vulnerabilities can be exploited by attackers [CIS19]. Some known cyber threats against UAVs and IoD are explained in Section 3.3.2.

There are several definitions of cybersecurity. According to Cybersecurity & Infrastructure Security Agency (CISA), cybersecurity is "*the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information*" [CIS19]. The International Telecommunication Union (ITU) provides a longer definition: "*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability, integrity, which may include authenticity and non-repudiation, and confidentiality*" [ITU].

[8] https://www.aviant.no/

3.3.1 Security Concepts

Common for both definitions is the focus on the security concepts Confidentiality, Integrity and Availability (CIA), called the CIA triad, which are known as the pillars of cybersecurity. Three other concepts are often shown to be equally important, namely non-repudiation, authenticity, and privacy. These six requirements are essential when it comes to security and privacy preservation in UAVs and IoD [YWY+22]. William Stallings [Sta17] provides an explanation of the six concepts:

- ◇ **Confidentiality** - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information, and preventing unauthorized disclosure of information.
- ◇ **Integrity** - Protection of information against improper and unauthorized modification or destruction, including ensuring information non-repudiation and authenticity.
- ◇ **Availability** - Ensuring timely and reliable access to and use of information.
- ◇ **Non-repudiation** - Provides protection against denial by one of the entities involved in a communication of having participated in all or a part of the communication, i.e. prevents either sender or receiver from denying a transmitted message.
- ◇ **Authenticity** - The property of being genuine and being able to be verified and trusted. This means verifying that users are who they claim they are and that each input arriving at the system came from a trusted source.
- ◇ **Privacy** - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

3.3.2 Cybersecurity Threats

The listed cybersecurity threats can happen for a single UAV as well as for IoD. The consequences can have a different impact on IoD since the IoD architecture contains several UAVs.

Spoofing

Spoofing is a cyberattack where false data injection is the goal of the adversary. As civilian GPS signals are unencrypted and unauthenticated, the GPS is vulnerable to spoofing attacks. GPS spoofing against a UAV is when fake GPS signals are sent out to change its navigation. An adversary can get complete control over the UAV when spoofing the GPS signals. [HAR22]

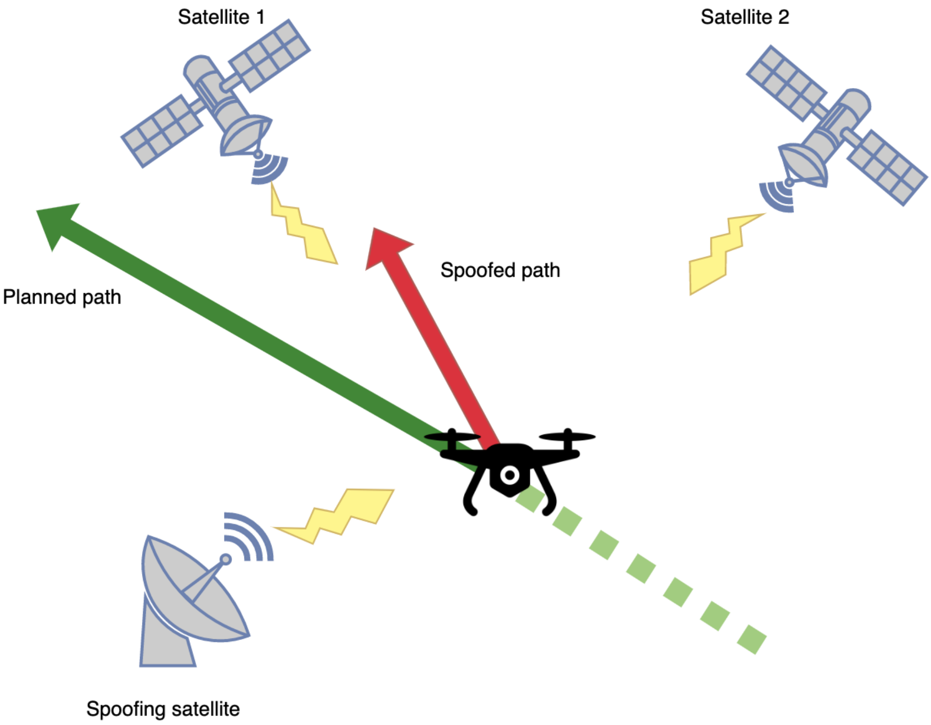


Figure 3.5: Illustration of GPS spoofing (adapted from [HCA+21a])

Jamming

As UAVs rely on the electromagnetic spectrum to receive commands, they are vulnerable to jamming. That is, intentionally or unintentionally directing electromagnetic signals towards a UAV [Kal22]. When it comes to UAVs, GPS jamming is among the most common. Here, distracting signals are directed toward the UAV as an obstacle to prevent it from receiving and decoding the normal signals. The consequences can be that the UAV becomes disoriented and disconnected from the GCS [HAR22].

Eavesdropping

Eavesdropping is a passive attack where the attacker listens to the communication without modifying it. The goal is to capture important data like encryption keys or even unencrypted data. [TGV22]

Man-in-the-Middle

Man-in-the-Middle (MITM) is an interception attack where an adversary places himself between two communicating entities. In IoD, the adversary will typically place a malicious UAV between the GCS and a victim UAV. The adversary can eavesdrop on the communication and modify the data from the sender before he forwards it to the recipient. He can masquerade as the GCS and relay false instructions, or even control the victim UAV. [YWY+22]

Denial of Service

DoS is a common cyberattack that can be used to stop a UAV from functioning normally [HCA+21a]. It affects the system's availability and aims to prevent legitimate users from accessing a system. This is usually done by flooding the network with packets, resulting in a congested network. A DoS attack directed at a UAV may result in the pilot not being able to perform wanted actions. Such attacks can also cause de-authentication between the GCS and their UAV connection [WA19].

Hijacking

Hijacking means taking control of the UAV, and many cyberattacks can lead to hijacking of UAVs in one way or another. GPS spoofing and MITM are hijacking by directing the UAV to the desired location. De-authentication can lead to an attacker obtaining control of a UAV flying nearby, thus hijacking the UAV. To accomplish this, the attacker has to be within the wireless perimeter of the UAV. The attacker utilizes the Medium Access Control (MAC) address of the victim UAV and disconnects it from the GCS by sending de-authentication packets [HCA+21a]. The attacker can then get control of the UAV by authenticating himself and connecting it to his controller [HAR22]. De-authentication is feasible on UAVs using WiFi and is possible because of security problems related to WiFi protocols.

Replay Attacks

Another cyber threat to UAVs is replay attacks. In such attacks, an adversary listens to the secure communication between the GCS and a UAV. Instead of decrypting the messages, he re-sends a message to the GCS to make it seem like he is the other communicating party. The GCS might continue to relay messages to the adversary instead of the intended UAV, thinking he is the original sender. [TGV22]

Information Collision Attacks

In an IoD network, many UAVs fly in coordination with each other. If several UAVs operate at the same frequency, information collisions can occur and the network can be perceived as unstable. Usually, collisions between one or more UAVs happen because of limited computing resources and inferior communication. [YWY+22]

Selective Forwarding

Malicious UAVs can occur in an IoD network. These can perform selective forwarding attacks by selectively dropping sensitive or important packets. These attacks are typically most productive when the malicious UAV is included in the data stream's path. As such attacks have the potential to drop or interrupt any kind of packets, the result can be an unreliable IoD network. [YWY+22]

Tampering Attacks

In tampering attacks, data is deliberately destroyed or altered by attackers through unauthorized IoD channels. It is possible to intercept and alter data while it is in transit or at rest. An attacker can intercept a data packet sent over an unprotected IoD channel, modify its contents, and change its destination address. Tampering attacks primarily violate the integrity of the IoD network. [YWY+22]

ADS-B Attacks

ADS-B lacks several security mechanisms and hence is prone to a variety of attacks. ADS-B signals are unauthenticated, meaning that they can be sent by unauthorized entities. They are also unencrypted, leaving them vulnerable to eavesdropping [Cos22]. There is no message integrity check either, so ADS-B messages can be deleted or modified [YMB+19]. Such signals can also easily be jammed or spoofed [HAR22]. In an ADS-B spoofing attack, the attacker targets the ADS-B ground station and aims to manipulate the International Civil Aviation Organization (ICAO) address in ADS-B messages. By doing so, the attacker can pretend to be a legitimate UAV or even create a false appearance of a non-existent one, a so-called "ghost UAV". As a result, pilots or ATC personnel can be confused, and dangerous situations can arise [YMB+19]. [OH22]

3.3.3 Threat Actors

It is important to understand the perpetrators behind the cyber threats we face today. As technology advances, so does the hackers and their methods [Haw21]. We divide threat actors into three categories based on their means:

Category 1

In the first category, we find people who do not afford a lot of advanced equipment but usually take advantage of publicly available tools and cheap tangible resources. They normally use pre-existing code to launch their attacks [DNV22]. Typically, you will find so-called “script kiddies” or “hobbyists” here, who may perform hacking activities as a hobby. Their motivation behind attacks can be curiosity or to demonstrate how skilled they are. Common in this category is that people are not educated in cybersecurity and attack techniques, and do not have a lot of means. Despite this, their attacks can have serious consequences [Rin19].

Category 2

In the second category, we find people who have money to buy means to use in their hacking activities. They know what they are doing, and have a goal with their hacking activities [KS21]. They are often referred to as “cyber criminals”. Organized hacker groups fall into this category [CIS]. In this category, the hackers are typically motivated by a monetary gain, either by performing ransomware attacks or acquiring information to sell. This is often called “hacking-as-a-service”, and they often target governments and organizations [KS21]. Furthermore, some hackers can be motivated by political, social, or environmental purposes. Such hackers are often called “hacktivists”, a combination of “hacker” and “activist”. With the rising concern for climate change, critical infrastructure can be targeted by hacktivists, especially the oil and gas industry is prone to this [MM20].

Category 3

The third category contains people who have a lot of resources, e.g. funded by a state, and use expensive and advanced tools and equipment to perform attacks. They have the means to hire the most competent people. Nation-state actors belong to this category, and political objectives like critical infrastructure sabotage and espionage on other countries and organizations are not unusual. [CIS]

3.4 Critical Infrastructure

Critical infrastructure is a common term for structures and functions that are vital to society functioning normally [Leh22]. Countries have different definitions of what critical infrastructure is, but common in almost all definitions is that it encompasses industries and companies that provide fuel, medical care, energy, telecommunication services, financial services, food and water, and transportation [Sto22]. A failure or disruption of such services could lead to severe repercussions on society, and impact citizens negatively in the means of health, safety, and prosperity. Critical infrastructure is subject to natural disasters, accidents, and deliberate attacks [Leh22].

3.4.1 Cyberattacks to Critical Infrastructure

Over the past years, there has been a rapid increase in attacks targeting critical infrastructure. The attacks have become more complex, and the attackers have become more professional, with the objective to disrupt the services. Today, automated IT systems manage and monitor both critical civilian and military infrastructure [Ted21]. Therefore, many of the attacks are targeting digital systems. Physical damage to the infrastructure is also present [Leh22]. An example of a physical attack was in November 2022 when Russia attacked the Ukrainian energy infrastructure, leaving millions of Ukrainians without electricity, water, and heat for weeks. The damage was caused by missiles and UAVs [HRW22]. However, this is not the first time Russians have conducted attacks on the Ukrainian critical infrastructure, according to the Ukrainian and US governments. In 2015, three electricity distribution companies in Ukraine experienced a cyberattack. Their control centers were accessed remotely and breakers were switched off, resulting in power outages affecting hundreds of thousands of Ukrainians [PW17].

Cyberattacks on critical infrastructure have huge consequences and there is a growing threat. The severity of the consequences depends on the industry. One of the top three industries reporting cyberattacks is the energy sector. For companies in the oil and gas industry, environmental damage could be more of a concern, while in power and supply, the biggest concern is disrupted operations. According to research done by DNV,[9] energy professionals anticipate that cyberattacks on the energy industry can compromise life, property, and the environment within the next two years. [DNV22]

3.4.2 The Role of UAVs in Critical Infrastructure

It is a major challenge to protect and optimize the critical infrastructure in the best way possible [Ted21]. To face this, UAVs have been applied to several industries within the critical infrastructure sector, where they can provide monitoring and maintenance on the critical infrastructure systems. The adoption of UAVs for this purpose has increased significantly over the past years. According to market research published February 2023 [Mar23], there is rising usage of UAVs as Remote Visual Inspection (RVI) tools for critical infrastructure applications. They are popular in the asset management sector due to their various benefits. The Compound Annual Growth Rate (CAGR) from 2022 to 2027 is estimated to be 14.6% [Mar23]. CAGR is the mean annual growth rate of an investment over a period of time, with a minimum of one year [Way22]. The increasing demand for safe and precise inspection and monitoring, as well as a reduction in costs and human safety, are the key market drivers for the UAV inspection and monitoring market [Nor22]. An example is using UAVs instead of exposing people to heights or voltage during inspections. UAVs also ensure greater timeliness of intervention [Ted21] and better accessibility [Nor22].

[9] https://www.dnv.no

For inspection of infrastructure, such as airports, highways, railroads, windmills, bridges, pipelines, or power lines, UAVs can be useful [VNBC16]. UAVs can detect weak spots, erosion, and attrition with cameras. Oil and gas facilities can use UAVs to inspect the platforms [Ted21], or to detect if pipelines are leaking gas or water if they have appropriate sensors. UAVs can inspect high objects from a close distance, like roofs, windmills, and electricity network cables [VNBC16], and they can also be used to check the status of maintenance and do transportation between different installations [Sto23b].

A concern related to monitoring and inspection of critical infrastructure using UAVs is that sensitive location data like photos or coordinates are transmitted [YWY+22]. Other concerns are related to safety when it comes to UAVs causing harm due to harsh weather conditions, bad flying skills, or cyberattacks [Nor22]. Aviation is critical infrastructure that will be massively disrupted by unauthorized UAVs. However, an integrated airspace consisting of both manned and unmanned aviation can enable the next phase of evolution for the aviation industry. An application of UAVs applied in aviation is BLoS operations. [Ale23]

3.4.3 Real-World Incidents Highlighting the Threats

In recent years, there has been an increase in the number of unauthorized UAV observations in Norway and over the Norwegian continental shelf. Among these are occurrences around airports and oil and gas facilities. Big UAVs with a wing span of several meters have been observed, and the Norwegian police suspect that a state actor is operating them, as they are very expensive and rare to get hold of. The UAVs are probably used for surveillance, which raises an intelligence threat and the need for a better anti-drone strategy. [Sto23c]

After Russia invaded Ukraine in February 2022, UAV observations in Norway have become more common [Sto23c]. From 2020 to 2021, no observations on the Norwegian continental shelf were reported to the police. However, from July to December 2022, the Norwegian police received 395 reports of UAVs, 115 of these from the Norwegian continental shelf [Sto23a].

2. December 2021, a UAV was observed around Sola Airport in Stavanger. The UAV had a wing span of minimum two meters and forced the airport to shut down several times due to its repeating appearance. The airspace was closed to prevent dangerous situations. In 2018, the North Atlantic Treaty Organization (NATO) exercise called Trident Juncture was held in Norway. At the time of the exercise, many unknown UAVs appeared around the operating area and Røros Airport [Sto23c]. These incidents were an awakener for the airport industry, and Sola Airport now has installed a drone detection system. Oslo Airport Gardermoen also has a drone detection system that has been operated since the 1st of April 2022. According to

Mats Gjertsen in Avinor,[10] the technology for detection of UAVs is still not mature. Some systems struggle with detecting everything, and other systems give false alarms. It is a complex technology [Sto23d].

5th of August 2022, the Norwegian oil and gas company, Equinor, contacted the police regarding unauthorized UAV observations on their offshore facilities. A UAV had been flying under one of the installations on the Johan Sverdrup field in the North Sea. This was a violation of the safety zone of 500 meters radius around the installation. After the media wrote about this, many cases of unauthorized UAV observations have been reported [Sto23b]. The Norwegian Police Security Service states they have no grounds for implying that Russia is behind the observed UAVs [Sto23e].

According to drone expert Nils Håheim-Saers, all we can do is wait until the state actors that do not wish us well start using UAVs to attack critical infrastructure. He thinks there is reason to believe that it will happen on bigger scales than before, where it harms us the most. Iranian UAVs has been used for years to inflict damage on the Saudi Arabian oil industry. Håheim-Saers warns about the fact that attackers can use the same Iranian UAVs to cause damage against our oil industry on the surface in the North Sea, as well as attacking the infrastructure on the seabed with other Autonomous Underwater Vehicles (AUVs). [Sto23d]

3.5 Relevant Case Studies and Incidents

In this section, material with relevant case studies is presented. First comes an explanation of how easy it can be to make a commercial UAV carry a dangerous payload, followed by a “ghost UAV” attack on ADS-B. Then, some attacks on military UAVs are discussed, and lastly, the capture of a police UAV.

3.5.1 Making a Commercial DJI Drone Deadly

In the YouTube video, “Drone Darts are Silent and Deadly!”[11] it is showcased how a normal DJI UAV is transformed into a weapon. DJI UAVs have the ability to turn on and off lights. With this in mind, it is possible to make a claw mechanism that reacts to the light being turned on by a remote controller. This mechanism can be built with Arduino Uno, a server motor, and a light sensor. The code for this program can be downloaded from the Internet and modified to suit the purpose. The server motor will be programmed to open and close. The solution needs to be small and light to suit the UAV payload capacity. To achieve this, one can create a circuit board and put it into a 3D-printed cradle, which then can be attached to the

[10] https://avinor.no/

[11] https://www.youtube.com/watch?v=969XGZ_t7cE

UAV. The cradle positions the light probe right in front of the UAV's hole containing the dart. Turning the light on and off moves the built latch which will release the payload, namely the dart. [Ale21]

The homemade solution turns out to be imprecise. Ideas for a more precise hit of the target is to rely on the GPS to position the UAV. The UAV was tested to hit a plate and a car. From 50 meters, the dart missed the plate with a foot. In the car scenario, it hit the car and went through the metal roof. The next test scenario was from 100 meters above, and the dart went through the car window, got caught in the metal frame of the seat and the windows were smashed into pieces. Later, it was sent from 100 meters. The darts went through the front window and would have hit the driver if there was one. From 200 meters above, the wind made the dart land far away and it was hard to aim. [Ale21]

This example shows how accessible information is on the Internet and how one can use this to enable malicious features on UAVs.

3.5.2 Ghost Injection Attack on ADS-B Equipped Drones Impact on Human Behavior

A ghost injection attack happens when an adversary transmits spoofed ADS-B to make it seem like a legitimate aircraft sent them. Such ghost aircraft can cause confusion between pilots, ATCs or UAVs operators. In the worst scenarios, this can make flight plans change, deny or force landings, and change of altitude and velocity. Haddad et al. [HOM21] performed ghost injection attacks to see how pilots and operators reacted, without letting them know beforehand that an attack would be carried out. This was done with a flight simulator using UAVs, and Haddad et al. created messages indicating that there was an aircraft close to the UAV. The ADS-B IN captured the messages, which were analyzed by the UAV software, and the pilots were notified if there was a risk of collision. The mission was to transfer organs to a hospital, and the pilots were aware that this was a time-critical assignment. This could have affected how they acted. The results from the study showed that almost a fifth of the participants did not bother about the notifications and continued the mission even after three alarms. Further, 15 participants landed after the first alarm and 5 after they received the second alarm. This demonstration shows that there are indeed means to say that ghost injection attacks make UAV operators abort their missions and can disrupt operations. [HOM21]

3.5.3 Military Attacks

In 2009, US soldiers found American intercepted video footage recording UAVs on devices owned by Shiiti fighters in Iraq [RBJ20]. Fighters in Iraq used a Russian program called Skygrabber. Skygrabber costs $29 and allows interception of packet radio service from a computer connected to a small satellite [Vac17].

In September 2011, a “keylogging” virus infected the United States UAV fleet at Creech Air Force Base in Nevada [HS13]. On December 2011, an American RQ-170 Sentinel drone was captured by Iranian forces, claiming they had sent false GPS signals to get it to land [Kal22]. An RQ-170 Sentinel is a newer type of UAV that can operate autonomously, and hold weapons. In 2012, Iranian forces were able to capture an American ScanEagle drone and mass produce it [HS13].

In the ongoing war between Ukraine and Russia, both sides use UAVs, both for reconnaissance and as weapons. As seen in Section 3.5.1, it is relatively easy to make a dangerous weapon of a commercial UAV. Aerorozvidka[12] is a team of civilian IT experts that is developing custom UAVs and modifying consumer UAVs for the Ukrainian security and defense forces [Com].

There is also a growing concern about autonomous weapons as it scales into drone swarms. Autonomous detection of enemies could be implemented with artificial intelligence. As these drone swarms grow in size, weaknesses in artificial intelligence can result in drone swarms becoming weapons of mass destruction in the future. Cyberattacks could disrupt UAV operations, make them crash, collect information on future attacks, and redirect UAVs to attack-friendly targets. These accidents show how vulnerable military UAVs are. [Kal22]

3.5.4 Hacker Reveals $40 Attack that Steals Police Drones from 2km Away

In 2016, researcher Nills Rodday at IBM figured out a way to hijack and steal a UAV belonging to the police. The UAV had a cost of approximately $30 000, and with equipment worth $40 and some knowledge of radio communication, he was able to compromise the UAV. The UAV was controlled with Android tablets and equipped with XBee ZigBee Radio Frequency (RF) chips. As the tablets did not have a corresponding chip, the WiFi signals were transmitted from the tablet to an intermediary that supported both WiFi and RF, transformed to RF, and relayed to the vehicle, and the other way around. [Rus16]

The chips on the UAV supported encryption, but it was not activated as this affected the performance. WEP was used as the WiFi protocol, which is known to have several security flaws. Within a perimeter of 2km, Rodday was able to perform MITM attacks and relay his own commands between the UAV and the tablet as well as dropping packets, gaining control of the UAV. [Rus16]

[12] https://aerorozvidka.ngo/

3.6 Attacks on Similar Systems

This section presents explanations of some attacks to similar systems like Unmanned Surface Vehicles (USVs) and the IoT. It is relevant to look at USVs because they can operate autonomously, and are therefore subject to many of the same attacks as UAVs like for instance GPS/Global Navigation Satellite System (GNSS) spoofing and Address Resolution Protocol (ARP) spoofing. As IoD is sometimes called "the Internet of Flying Things" [JZR22], it is interesting to look at attacks that have targeted IoT systems as well.

3.6.1 Internet of Things

IoT is one of the enabling technologies for IoD [CYK+21]. The integration of IoT and UAVs can rise some security challenges. Some threats to IoT are spoofing, sniffing, key logging, information gathering, and signal jamming [HCA+21b]. These risks will influence the IoD domain as well.

It is possible to use Shodan Search Engine[13] to search for IoT devices. With Shodan, it is feasible to find out the software version of devices connected to the Internet, and hence vulnerable devices that are not yet patched to the latest version. In order to keep you safe, Shodan offers a thorough overview of all exposed services.

Several attacks targeting IoT have been carried out. Two well-known are discussed below.

The Mirai Botnet

Mirai is malware that was used to target and infect vulnerable IoT devices. It took advantage of weak security configurations like default credentials and used compromised devices to launch Distributed Denial of Service (DDoS) attacks. At most, there were over 600 000 IoT devices infected by Mirai. A number of enslaved devices could be rented out to take part in DDoS attacks. Three major DDoS attacks took place, two of them against Internet Service Providers, forcing popular services like Netflix and Twitter to go offline for around two hours. [Eus19]

The Jeep Hack

In 2015, a group of hackers were able to demonstrate the remote hijacking of a Jeep. They were able to turn on the fans and the stereo, lock the doors, disable the breaks, and steer it if the car was below a certain speed. This attack was possible since the car was connected to the Internet, and is a growing concern as more cars are becoming connected to the Internet. [WIR15]

[13] https://www.shodan.io/

3.6.2 Hijacking of USVs

The state of art and related work were reviewed, and an identification of the relevant background material was carried out in the project preceding this thesis [OH22]. No relevant new material was found during the work on the thesis. The information from the project report is included below.

USVs have a lot in common with UAVs considering the technological aspects and use cases. They are highly attractive targets by adversaries, and many of the cyber threats they are prone to, are relevant for UAVs too. USVs are mainly autonomous ships that provide services in a similar manner to UAVs, such as remote surveillance, mapping, and environmental monitoring. Solnør et al. [SVG+22] demonstrated that USVs are vulnerable to hijacking. By spoofing the ARP, which purpose is to link IP-addresses to MAC-addresses, the attacker redirects the traffic through his device. This is because the IP-address of the intended receiver is now linked to the MAC-address of the attacker's device. The attacker can modify the transmitted data before it is forwarded and may send the vehicle in the wrong direction. Such an attack may be performed on a UAV too, changing its course. [SVG+22]

3.7 Mitigations

Protecting an IoD environment requires the implementation of various cryptographic methods, key management, authentication, access control, intrusion detection, and preservation of privacy. [BCD20]

3.7.1 Access Control

Access control is an important security measure that is essential to secure data in an IoD environment as well as in an IoT environment [BCD20]. Chaudhry et al. [CYK+21] proposed a certificate-based Generic Access Control Scheme for the Internet of Drones (GGACS-IoD). With GGACS-IoD, every UAV and GCS obtains an initialization certificate by registering with a control room, before any communication will start [TGV22]. The certificate makes sure the UAVs are only allowed to join the IoD after being fully initialized. GGACS-IoD protects against insider attacks since registration data can not be accessed before deployment, and provides authentication in the IoD domain. It also protects against impersonation, MITM, and replay attacks.

3.7.2 Collision Avoidance

Kumar et al. [KKN+21] proposed a system for UAV collision avoidance strategy with specific UAV movement and collision avoidance algorithms. The system makes the UAV able to select either single-layer or multi-layer UAV movement strategies. In a single-layer approach, the UAVs will move at one height only. They can use a

RADAR/Light Detection and Ranging (LiDAR)-based approach to avoid collisions or select a pre-defined zone-based movement and collision avoidance strategy. Both RADAR and LiDAR aim to detect objects, but LiDAR uses a laser to measure distance while RADAR uses radio waves [Nea18]. The ability of UAVs to fly in three dimensions and execute intricate flight patterns increases the difficulty of determining their arrival and departure times within the coverage area of IoD [TYS19]. This system can protect against collisions.

3.7.3 Lightweight Authentication

A UAV has limited space and hence limited battery power, so it requires lightweight authentication techniques. Srinivas et al. [SDKR19] designed a novel Temporal Credential-Based Anonymous Lightweight Authentication Scheme (TCALAS) for the IoD environment. TCALAS applies a one-way cryptographic hash function and fuzzy extractor for biometric verification which is based on temporal credentials. All participants in the IoD network can efficiently implement this mechanism. In a fly zone, which can be interpreted as a cluster of UAVs, the UAVs will communicate with each other and with the GCS. If an external user is able to access the UAVs in the fly zone, he can monitor them using his own mobile device. Before any services are provided, all UAVs must register with the GCS, which is the only trusted entity in the IoD environment. The mechanism has proven to resist various attacks like for instance MITM and replay attacks. [SDKR19]

3.7.4 Cryptography-Based Authentication

A cryptography-based authentication scheme using Elliptic Cruve Cryptography (ECC) and symmetric key primitives was proposed by Hussain et al. [HCA+21b]. The proposed solution protects the communication between a user and a UAV using three-factor with the user's mobile device, password, and biometrics. The GCS serves as an intermediary agent in the sharing of session keys between UAVs and the user. Both the user and the UAV authenticate each other before a session key is shared, called mutual authentication. This scheme provides confidentiality by providing secure user access to the UAV on a public channel and protects against impersonation and some DoS attacks. [HCA+21b]

3.7.5 Privacy-Preserving Authentication

To address security and privacy concerns in IoD, Tian et al. [TYS19] proposed an efficient privacy-preserving authentication framework. The framework ensures efficient authentication during deployment on resource-constrained UAVs, through the use of a lightweight online/offline signature design. The signature design involves fast modular arithmetic operations for each UAV under authentication. Privacy is an important cybersecurity aspect, and this solution incorporates privacy protection for

UAVs by safeguarding their identity, location, and flight paths. Non-repudiation is also provided by the means that a user cannot deny what he has done. The efficiency of the security services offered in the framework is guaranteed with the assistance of Mobile Edge Computing (MEC). [TYS19]

3.7.6 Blockchain-Powered Solution

Blockchain offers benefits when it comes to the design of security mechanisms for the IoD environment [YWY+22]. With blockchain, data is stored on several different nodes, making the data storing decentralized. In addition, blockchain makes use of cryptography to secure transactions. Bera et al. [BCD20] designed a secure blockchain-based access control scheme for IoD deployment. This scheme allows secure communication between UAVs, and between UAVs and the GCS. Data collected from the GCS form transactions and those transactions are transformed into blocks that are added to the blockchain. The blocks are then added to the blockchain through the Ripple Protocol Consensus Algorithm (RPCA). This process occurs in a peer-to-peer network of cloud servers connected to the blockchain. After the blocks are added to the blockchain, the transactions contained within them cannot be altered, modified, or removed. The proposed solution can mitigate attacks like replay, impersonation, MITM, privileged-insider, and physical UAV capture attacks.

3.7.7 Intrusion Detection

An Intrusion Detection System (IDS) is either a device or a software application that is designed to detect any unauthorized access or privacy invasion to the targeted network [YWY+22]. Ramadan et al. [REAE21] introduced a real-time data analytics framework for IoD intrusion detection based on deep learning. The framework is based upon Recurrent Neural Networks (RNN) and involves the collection of data from the network. This data is analyzed using Big Data analytics for anomaly detection. Each UAV will have one module that will try to detect attacks on the UAV itself. Another RNN module will reside at the base station and confirm the attacks and notify other UAVs of other attacks [REAE21].

3.7.8 Protection of Cloud Data Privacy

In order to protect the privacy of cloud data in the IoD, Chen and Wang [CW19] introduced a network coding-based pseudonym scheme. The use of pseudonyms can help preserve user privacy. The design of the two-tier scheme allows for the separation of IoD cloud data from the owner's pseudonyms. The solution is implemented when facing untrusted cloud databases and can defend against both inside and outside attackers. The outside threat is mitigated by having ciphertext that cannot be broken with infinite computation time, and to decipher the complete ciphertext, an attacker has to attack all the nodes. The inside threat is mitigated by decoupling data ownership so the insider attackers do not know about the relationship between the stored data and the owners. [CW19]

3.7.9 Detect ADS-B Spoofing

To detect ADS-B spoofing attacks, Ying et al. [YMB+19] introduced a two-stage Deep Neural Networks-based spoofing detector. The detector is composed of two classifiers, one for messages and the other for aircraft. By analyzing the incoming messages based on the PHY-layer features, the GCS can identify suspicious messages. Results from the experiments described in the paper show that the solution detects ground-based spoofing attacks with a 99.34% percent probability and also has a small false positive rate. [YMB+19]

3.7.10 IoT Security Checklist

As the IoD is an extension of the IoT, many of the security measures to IoT apply to IoD. SINTEF has created a checklist of questions aimed at raising awareness and assessing the security of devices in an IoT network. The checklist can be used to evaluate the security level of UAVs as well. The questionnaire includes various aspects such as checking for encryption, automatic software updates, avoidance of hardcoded credentials, employing a secure wireless communication protocol, mutual authentication, and mechanisms for detecting malicious or compromised devices. [SIN22]

3.8 Our Contribution

A gap was found during literature studies for our project, with regards to security aspects related to the use of IoD in critical infrastructure [OH22]. It does not seem that this is something that has been addressed before. It exists limited research in the area of security of the IoD. We want to address what cyber threats exist for critical infrastructure operators when using IoD for inspection and monitoring, and what can be done to mitigate the risks.

Chapter 4 Interviews

In this chapter, our findings from the interviews are presented. First, some information is provided about what the connection is between our interviewees and UAVs. Then, the benefits, limitations, and future outlooks of UAVs that were found during the qualitative analysis are presented. The same structure follows for the IoD. In addition, the use of IoD within the critical infrastructure is discussed. Furthermore, a section about cybersecurity threats and mitigations to the proposed threats is presented. All the results presented in this chapter have been anonymized. See appendix A for the interview guide.

Interviewee 1 and 6 work in a research organization and Interviewee 2 is a researcher in the UAV field. Interviewee 3 works with countermeasures against UAVs. Interviewee 4 has a high position in a company that provides UAVs for various services. Interviewee 5 is a drone operator in a conflict area, and Interviewee 7 works in a company providing UAV services.

4.1 UAVs

4.1.1 Benefits

Interviewee 1 explained that there are several benefits to using UAVs, particularly in logistics. UAVs can be used to quickly deliver goods, save costs, and have a positive impact on the environment. For example, drone delivery can in some cases be more energy-efficient compared to traditional delivery methods such as driving. However, the cost-effectiveness of drone delivery is still a topic of debate, especially when compared to established transport companies that have many deliveries on their routes.

Interviewee 2 listed several benefits of using UAVs, including their quickness, ability to replace people in dangerous areas, and usage in military applications such as continuous surveillance and security patrolling. ScoutDi,[1] which offers a tethered drone system, was mentioned as an example of a company where UAVs can enter where you don't want people to do repetitive work. UAVs are also useful in dull, dirty, and dangerous environments, which they were initially built for, although they may not necessarily be cheaper than other solutions. Overall, UAVs are seen as a safer option for people, but not necessarily for a lower cost.

According to Interviewee 3, UAVs are a good supplement to helicopters as they can easily elevate and get a bird's eye view. UAVs are relatively easy to use and there are many UAVs available compared to helicopters, making them a cheap, quick, and effective way to get an overview of a situation. Another benefit of using UAVs is that the information captured can easily be shared with others, creating a common situational understanding early on.

Interviewee 4 first mentioned that UAVs are beneficial for internal business operations such as the media and press companies, energy providers, and physical infrastructure constructors. These companies have been using UAVs for several years to create map backgrounds and collect inspection data in a cost-effective and efficient manner. For instance, using UAVs for line inspection eliminates the need for people to climb masts, or use scaffolding or safety equipment. Using small electronic UAVs is primarily cheaper than using a manned helicopter according to Interviewee 4. Secondly, UAVs can provide high-quality data that can be useful for the services provided.

The benefits of using UAVs in military operations were discussed by Interviewee 5. According to the interviewee, UAVs are effective in providing detailed intelligence for getting a proper overview of the front line, which is not possible using standard observation methods. It was also mentioned that artillery launches are more effective with UAVs because they can hit the target precisely. However, the biggest benefit highlighted was the ability of UAVs to help save scout lives by avoiding the need to send people to do observations close to enemy positions. Instead, UAVs can be deployed to capture a comprehensive visual record of the surroundings.

Interviewee 6 talked about using UAVs to get a situational understanding of places where it has been avalanches, landslides, or similar incidents. A UAV can share video footage with the police and defense if needed from different perspectives. "*If a doctor gets access to pictures from the area where a disaster has occurred, the doctor could wish to see something different than the police and fire department*" - Interviewee 6. The doctor would want to search for injured people, while the police might want to see if anybody is leaving the area. A UAV can play several parts in such situations, but the challenge arises when it comes to sharing the requested

[1] https://www.scoutdi.com/

information from a single UAV to all the agencies that require it.

4.1.2 Limitations

Interviewee 1 pointed out that UAV operations in cities will have a safety and noise perspective. There are also weight and payload restrictions.

Social acceptance of UAVs and the fact that the mature technology is limited, were limitations provided by Interviewee 2. The regulatory framework was mentioned as a limitation by Interviewee 2, 3, and 4. The allowed height, weight restrictions, and no-fly zones fall under this. Interviewee 3 also mentioned weather conditions and the battery, as it will get drained and hence limit how long you can fly. Moreover, the UAVs have limits on how far away from the controller they can fly.

When it comes to a communication perspective, Interviewee 5 mentioned that UAVs are limited by technical characteristics like signal strength and distance. Interviewee 6 pointed out that a UAV using mobile communication would see several base stations when in the air. Research has shown that the base stations would try to connect to the UAV because it is an available terminal, which it would experience as interference. Another thing is that it would be arbitrary if the UAV has a connection to a base station or not, as the antennas on base stations often point down towards the humans, or laterally. For WiFi today, the performance is based on how many are using it, so it can be poor at times. It can be like that for UAVs over mobile communication as well. "*The coverage for drones that use 5G today is more or less like WiFi coverage. If it works, it works*" - Interviewee 6.

4.1.3 Future outlook

Interviewee 1 said that as the potential of UAVs continues to increase, so will the market share. For this to happen, there needs to be a development process with the interaction between the users, developers, and regulators.

Interviewee 4 mentioned that the former American president, Donald Trump, facilitated American and Western technology to get a competitive advantage. Parrot and Skydio[2] are examples of such UAV companies. The interviewee indicated that interest in non-Chinese, i.e., Western-friendly, produced UAVs will increase considerably.

In a conflict scenario, Interviewee 5 suggested that the use of AI with UAVs can be useful in future reconnaissance missions to automatically detect objects in offensive missions. This could be helpful where humans feed coordinates to the system and launch a stack of UAVs that could hit the target.

[2] https://www.skydio.com/

In the future, Interviewee 6 believed that UAV providers will deliver UAVs with integrated 5G systems, as 5G is the first mobile technology that is mainly developed for industrial applications. It provides lower latency, higher security, and more robustness, to meet the conditions of the industry. For 5G, you can buy a capacity and the telecom operator can guarantee coverage in certain areas. However, mobile coverage is not meeting the requirements of the industry yet. "*In the future, drones might be a service that telecom providers will want to facilitate. Then they must guarantee a certain coverage up to a particular height, as the UAV industry requires assurance that it works*" - Interviewee 6. A future function by using 5G for UAVs is that the network can be used to position the UAV as a backup for GPS. The interviewee has been in contact with a large telecom operator regarding this function, and they responded that they do not see a high enough customer base yet. The interviewee mentioned that they have an interest in pursuing further research in this area.

4.2 IoD

4.2.1 Use cases

Interviewee 1 pointed out that IoD could be useful in time-sensitive applications. Related to the earthquake in Turkey in early 2023, UAVs were used as spotlights, but with the IoD you would have a network of spotlights that could ensure better coverage. Interviewee 2 also mentioned that swarms of UAVs combined with other types of robots could be useful related to the Turkish scenario.

Further, entertainment was pointed out as an IoD use case by Interviewee 2 and 4. In entertainment, one could have light shows provided by multiple UAVs instead of fireworks. Interviewee 2 also mentioned the company Zipline, since they are using a swarm of UAVs flying on pre-existing routes, to deliver medicines. Out of all the applications, the inspection of infrastructure power lines was mentioned as the first one to come.

Interviewee 2 and 4 agreed that IoD could be useful in attack scenarios and in military purposes. Another application mentioned by Interviewee 1, 2, and 4 is the ability to cover large areas faster. This could be particularly good for search and rescue. Interviewee 4 saw a huge potential in gathering a large data collection in the case of large perimeter surveillance. For real-time inspection and mapping, it could be useful in cases where you need to capture data quickly in a limited area.

Interviewee 6 talked about environmental monitoring and goods delivery as application areas. Amazon is already looking at this, the participant said. Both Interviewee 1 and 6 highlighted that UAVs can operate as base stations and provide a communication network. It may also be that you can use it as a relay if you do not have coverage somewhere.

4.2.2 Benefits

Interviewee 1 summarized the benefits as being fast and time-saving. Also, it was mentioned that IoD could provide a more robust communication due to the many connected UAVs. If one UAV lose its signal, it could depend on another UAV in the network. This is something Interviewee 7 also highlighted. Furthermore, Interviewee 7 believed IoD would ensure fewer collisions of UAVs in the future because a network of communicating UAVs could be more robust than a centralized hub on the ground. Interviewee 2 saw the potential of individual UAVs combined into a single database. Interviewee 3 said that with IoD everything gets more robust and available, as well as increased performance and data capacity. By utilizing IoD you can get more out of the UAVs. "*IoD can contribute to the drone sector becoming a more common business, which makes it safer because standardizations and regulations will follow*" - Interviewee 6.

4.2.3 Limitations

Interviewee 2 said that a challenge with a swarm of UAVs is the ability to control them and fit into today's regulatory framework. The participant said there is a long way to make UAV collaboration in a way that actually helps and does not create more problems. Also, social acceptance of swarms would take years to establish. Interviewee 6 also had concerns related to collisions between UAVs in the air and how to avoid them, due to management challenges.

Interviewee 3 emphasized that the importance of ensuring that the companies deploying the IoD do not become more vulnerable than strictly necessary. A lot of things work well in demos and animations, but in the real-world other factors come into play that you have not thought of. Regarding autonomous UAVs that would operate with perimeter security, it is a case that will not happen before some years due to the regulatory requirements placed on aviation. "*It is an exciting thought that needs to be thought through twice. Are we ready? No, but it will surely come*" - Interviewee 3.

Interviewee 4 mentioned that people are working with IoD at several renowned universities and research organizations. The participant does not see that they can utilize the IoD technology before presumably 10 years. The regulations need to be incorporated first, and the interviewee particularly highlights the need for U-space regulations for how the shared airspace of manned and unmanned traffic should communicate with each other.

4.2.4 Future outlook

Interviewee 3 believed IoD is a promising technology, but there must be a net profit. Generally, the interviewee highlighted that there is a lot of innovation and money in IoD. The technology is running many years ahead of laws and regulations.

Interviewee 4 thought that the technology coming from IoD would be adoptable to U-space and digital flight routes. Units must position themselves in relation to each other and communicate. That is what we are missing between manned and unmanned, and unmanned and unmanned aircraft.

Interviewee 6 thought that 5G technology would mean that IoD is used to a greater extent. The interviewee saw an opportunity for the telecom operators to define how IoD would be exploited as it is a growing market. There is potential upside in making it possible for start-ups or new businesses to build industrial IoD applications that make use of what their network can deliver. The more the telecom operators facilitate that their network can be used and support that type of service, the more such services will come.

4.3 IoD in Critical Infrastructure

Interviewee 1 guessed that it may be more appropriate with several UAVs to inspect, for example, one blade each on a windmill, as the blades usually are very large, and would take time to inspect. As a result, the inspection would consume less time, the windmill can be shut down for a shorter period and the energy company would lose less money since the wind turbine can more quickly get back to producing energy. Thus, the full potential of using IoD within critical infrastructure must be evaluated within each use case. "*I think it has a big value proposition within certain use cases*" - Interviewee 1.

Interviewee 2 said that the potential of using IoD for infrastructure protection is not there yet. A guess is that in maybe ten years from now we will see it, as there is not a posing threat at the moment. Further, it was mentioned that management of this would be hard, and there are risks that the UAVs may hit things they are not supposed to hit. In critical infrastructure, there can be zones that are flammable with explosives or gasses, where it is important that UAVs do not enter.

Even though Interviewee 2 stated that IoD is not mature for critical infrastructure, the participant saw that a single UAV could be very useful in certain areas and useless in others. They increase the inspector's safety since they then do not need to climb barriers. Secondly, there are UAVs that can fly and notice for example a gas leak due to sensors that are able to detect gasses. For power line monitoring, a UAV is very useful for quick intervention. "*The UAVs are very good companion* *tools. If you have a UAV constantly being on-site and reacting quickly, then it's a big change*" - Interviewee 2. The interviewee further mentioned that for railways and roads using UAVs, it is more about maintenance and the ability to map an area before construction. These are, according to the interviewee, cases for a single unit and would often not work for a network of UAVs.

From a resource and cost perspective and a safety and health perspective, Interviewee 4 believed that UAVs are very useful when it comes to the inspection of critical infrastructure. IoD can, for example, enable the lifting of heavy cargo by connecting several UAVs.

Interviewee 7 mentioned that IoD could be used to deliver spare parts to a critical infrastructure installation on short notice.

4.4 Cybersecurity Threats to UAVs and IoD and How to Mitigate Them

4.4.1 Threats

Many of the threats to UAVs are threats in IoD too, Interviewee 4 believed. An example is jamming as jammers are affordable and can impact both in a negative way. Jamming was mentioned as a threat to UAVs by Interviewee 1, 2, 3, and 6 as well. Interviewee 1, 2, and 6 specifically mentioned GPS jamming. All four mentioned GPS spoofing as well. "*GPS signals are very weak which make them easy to jam*" - Interviewee 6. Interviewee 4 mentioned that they have repeated incidents of GPS jamming. Interviewee 6 said that Russia emits a lot of noise to hide what they are doing, and this affects the GPS systems on flights in areas close to the Russian territory. Further, Interviewee 2 believed there is a risk that the data gathered by UAVs get into the wrong hands. Interviewee 7 mentioned MITM and GPS spoofing.

Regarding threats in conflict areas, Interviewee 5 mentioned DoS, radio spoofing, and emulation of no-fly zones for DJI UAVs. Also, drone guns[3] are a threat because they can shut down the video signal on a UAV. The operator would then lose the visual. Interviewee 5 further mentioned that these threats happen almost every day, and they lose UAVs very frequently.

According to Interviewee 6, it is hard for the UAV to verify whether the GPS signals are coming from a GPS satellite or not, since the signals are not authenticated. "*It is important that the drone can trust the signals it receives and operates on*" - Interviewee 6. This is especially important if the UAV is to do something for an industrial partner or a safety-critical operation. It was mentioned that military GPS

[3] https://uncrate.com/dronegun/

has authentication, but not civilian. Hijacking is also a serious threat, especially regarding critical infrastructure since there are many vulnerable systems. If a UAV is hijacked, it can be used as a weapon to cause damage. "*If a UAV is connected to the Internet, it can be hacked. Everything connected to the Internet is vulnerable*" - Interviewee 6. Interviewee 4 also said that hijacking is a potential threat, but that it does not exist much research in that field in relation to UAVs.

Interviewee 4 expressed concerns that the UAV market is dominated by the Chinese company DJI and that there are possibilities that the information gathered by the DJI UAVs is shared with the Chinese government. This is concerning, especially if DJI UAVs are used for the inspection of critical infrastructure. Interviewee 1 said that for certain use cases, Chinese-produced UAVs are not preferred. One does not want other governments to get insight into such sensitive data. "*The biggest threat right now is the lack of knowledge of what kind of information is shared*" - Interviewee 4. Further, Interviewee 4 shared that they experienced an unintended event when they did testing with a 4G ferry module that connects to the DJI UAV from a third-party supplier in China. During the testing, it turned out that the supplier was able to control the UAV, and this feature was not included in the technical documentation.

Interviewee 1 mentioned that the UAV itself can be a threat, and we have seen several airports being closed due to observations of unauthorized UAVs. Interviewee 5 mentioned that in Ukraine, UAV attacks are common because Russia is using military UAVs to destroy critical infrastructure objects and to perform chaos in residential buildings. That includes Russian and Iranian-produced fixed-wing UAVs that can carry kilograms of explosive loads.

4.4.2 Mitigations

Interviewee 1 and 2 mentioned that encryption is a requirement to overcome cyber threats related to UAVs. Interviewee 2 explained that one can have point-to-point encrypted communication and redundancy on navigation with some form of backup system. Interviewee 2 also said that if your UAV was to be captured, you would want to have encryption on the chips, so the perpetrator is not able to download the software from it. "*For example, when you make a code you can use obfuscation, which makes your code almost impossible to read in areas which you cannot protect*" - Interviewee 2. Other mentioned mitigations are to use VPN to access the UAV or change the credentials to a sufficient password. Interviewee 7 mentioned that they have their systems, for instance, the GCS and UAVs, on OpenVPN.[4]

[4] https://openvpn.net/

According to Interviewee 2, losing control of the vehicle can have severe consequences. A mitigation can be to carefully select the radio frequency used. Another mitigation to avoid getting hacked is to make sure you do not have any technical errors in your system. To protect yourself, Interviewee 2 said that you can build your design based on open-source which is tested by a community. Further mitigations mentioned were to remove access to the Internet when not needed, so you just stay in the internal network and have a fail-safe plan so you know what happens, for instance, if coverage is lost.

Interviewee 2 talked about using the integration of drone-in-a-box[5] technology into critical infrastructure monitoring. "*I think if someone or some company is not the producer of a drone, they don't have any control about what's in the box*" - Interviewee 2. This is an issue, and the interviewee had heard about a company that decided to pay around 100 or 1000 times more to develop a solution themselves, instead of buying a solution. This was because they did not trust the solution provided and they could not integrate it with their network. A solution is to keep it either completely as a separate box without access to your network or to integrate it. Then, if you decide to integrate you want to make sure your information will not be sold to third parties.

To ensure the security of UAVs in the future, Interviewee 2 said the first thing would be to see if there was an attack or data leak. People react to existing threats, not potential threats. For critical infrastructure, people will only use technology they can trust. In that sector, it is crucial that the technology function flawlessly since people are primarily concerned with its reliability rather than its novelty. Aviation, for instance, is a mature industry where the design is not changed even though the technologies are sometimes 50 years old. Aviation is a business of safety.

To protect the critical infrastructure against malicious UAVs, Interviewee 2 mentioned anti-drone systems and detection systems like Advanced Protection Systems,[6] which is a supplier that specializes in 3D radars for use in detection and neutralizing UAVs and is popular in existing conflict zones. Interviewee 6 also mentioned that big airports have systems to track a noise source that influence the GPS signal to find the source as fast as possible. There are also solutions provided by DJI themselves. There are hardboards that can be bought that know about all DJI UAVs in a five kilometers radius of your location. If an infrastructure operator has this type of solution and someone is flying around, they can send out a guided patrol that can reach the operator. This way the situation can be handled in a proper manner.

Regarding how organizations can react effectively to a UAV cyberattack, Inter-

[5] https://www.unmannedsystemstechnology.com/expo/drone-in-a-box/

[6] https://www.linkedin.com/company/advancedprotectionsystems/?originalSubdomain=pl

viewee 3 highlighted that it is important to think novel. What has worked in the past, will not necessarily work in the future with this emerging technology. The interviewee considered that when their company use UAVs, what the UAV sees is not only restricted to the company but can be seen by others as well. "*Everything that can be used can also be misused, and you have to be aware of that*" - Interviewee 6. This can be included in a risk assessment or vulnerability analysis to get a more conscious relationship to it. Further, it was mentioned that when 5G is a more widespread technology in UAVs, it might be harder to jam UAVs using 5G.

Interviewee 4 mentioned that there exist jammers that can send out a strong signal and influence the UAV so it will return to home, hold position or do what it is programmed to do. These jammers are directed, so they do not affect the WiFi in the neighboring house. Interviewee 3 also mentioned these jammers as a countermeasure against unwanted UAVs. It is further mentioned that the small DJI UAVs use frequency hopping, but that is quite easy to jam. For their bigger fuel-driven UAVs, they use encrypted links over a special radio network. To secure their UAVs even further, they always have them locked inside so they are physically unavailable to unauthorized people.

Interviewee 5 highlighted that the mitigations to DoS attacks are quite limited. It is possible to have specific antennas allowing to strengthen the signal and to avoid flying into a zone that is known to have drone guns in them. If the scenario is anti-aircraft warfare, there is not much to do except reconnaissance in the region and try to investigate where the equipment that is affecting the UAVs is located. For an attack by smaller drone guns, you can use your UAV in manual mode to be able to return them. It would not work with a civil drone in an automated mission, as an operator must control the UAV manually. A general mitigation mentioned by Interviewee 5 is to use UAVs on a non-standard frequency, not 2,4 or 5,8 GHz. To protect yourself from malicious UAVs it is also possible to apply a no-fly zone where you do not want UAVs. The interviewee mentioned that DJI broadcast the location of their UAVs and the coordinates of the pilots. One mitigation to hide this is to do modifications to these UAVs by using equipment that overrides the coordinates to zero. In a war scenario, this is necessary, otherwise, it would be less than 30 minutes until the location where the operator is sitting is exploited and possibly attacked.

Interviewee 6 said that some researchers working on navigation have built the world's largest database on jamming events on satellite signals. They have placed several sensors in different places in Norway and Europe. As soon as the sensors detect noise disrupting the GPS signal, on Galileo,[7] BeiDou,[8] and all other satellite-based signals, the data get dumped to a disk. Later, they can analyze the data to

[7] https://www.esa.int/Applications/Navigation/Galileo/Galileo_satellites

[8] http://en.beidou.gov.cn/

find out what type of jamming it was. The analysis can show what the most normal way of jamming is. Based on that, it is possible to make systems in the future that to the greatest extent possible can counteract the type of jamming that normally occur. "*It's also important to remember that jamming does not necessarily have to be an intentional act. All the electronics we surround ourselves with emit some form of noise*" - Interviewee 6. By knowing the general background noise in the area your system is supposed to be operating, you can build your system around it.

A countermeasure against spoofing mentioned by Interviewee 6 is to measure the signal strength and if it is too high, it is unlikely that the signal is coming from space. An algorithm could state if the signal is to be trusted or not. Interviewee 7 mentioned that GPS spoofing might not have too serious consequences on more advanced UAVs, as they would often have mechanisms to detect this, for example, by comparing the signals to the rest of the sensor input.

In interview 7 it was mentioned that all their autonomous UAVs have the opportunity to be remotely controlled and overridden by a backup pilot. The fact that they can be controlled by a pilot is a security layer. For an autonomous UAV it could be harder to detect if something has gone wrong, compared to a remotely controlled UAV where a pilot always monitors and detects faults more easily. According to Interviewee 7, the biggest challenge facing the UAV industry when it comes to securing UAVs against cyber threats is that everything is new.

When considering the balance required between security and the necessity to uphold the functionality and performance of the UAVs, Interviewee 7 stated that there is not much of that balance; when a UAV becomes safe enough, it is ready for use. It is a matter of definition to decide what is "safe enough". It was mentioned that their company uses encryption and that security is a prerequisite for everything they do. If a UAV cyberattack occurs, it was mentioned that they have emergency procedures in place. "*Having procedures in place in advance is the most important countermeasure. Preferably a couple of exercises*" - Interviewee 7. The mentioned step needed to secure the future UAVs is to keep the UAV and its integrity secure, as well as the keeping the GCS secure both physically and digitally.

Chapter 5 Experiments

This chapter explains the experiments, more specifically, how we chose the software, the setup, and the results obtained. We chose to perform GPS spoofing attacks. This attack was chosen because it appeared in the literature, as well as mentioned frequently during the interviews, which gave us an idea that this might be an attack that happens often. The experiments provided us with an idea of how realistic such an attack is and what the consequences could be.

5.1 Evaluation of Software

We found several programs that could be used to simulate UAVs, and we assessed the most promising ones in detail. They are further elaborated. One important evaluation factor was that it had to be possible to simulate multiple UAVs. We have not focused on exploiting the IoD in this thesis, as creating a communication algorithm ourselves was out of scope, and neither did we find one online that we could use. Thus, the multiple UAVs formed a swarm and not an IoD network. Moreover, a requirement was that a GUI had to be available to get a visual understanding of what happened during the attacks. Other important features were that the programs were worth using timewise and that GPS spoofing would be feasible. It was also important that it had an open license. Table 5.1 summarizes the characteristics of the most promising software evaluated.

5.1.1 BlueSky

BlueSky Air Traffic Simulator[1] is an open-source tool for performing research on ATM and Air Traffic Flows (ATF) developed by Delft University of Technology (TU Delft) in the Netherlands. It provides visualizations and simulations of traffic scenarios without any restrictions regarding licenses or other limitations. The program is written in Python and includes extensions for drone-specific traffic simulation [HE16].

[1] https://github.com/TUDelft-CNS-ATM/bluesky

A limitation we found with BlueSky was that the UAVs were difficult to program, as they were created and controlled with pre-configured commands that could be typed into the terminal. Hence, it was not suitable for performing GPS spoofing.

5.1.2 IoD_sim

IoD_sim[2] is a simulator for the IoD developed on top of NS3,[3] which is a well-known discrete-event network simulator. It is licensed under GNU General Public License. It provides communication between UAVs in a swarm [GIBG22]. To have a GUI, two other packages are required, Splash and Airflow [AGI+23]. As NS3 is used for network performance, a limitation with IoD_sim is that other attacks than DoS would be difficult and time-consuming to achieve, and therefore this software was not chosen.

5.1.3 Dronekit

Dronekit[4] is an Apache 2.0 Licensed Python package that allows the creation of apps that can run on drones. It is also compatible with Software in the Loop (SITL), a method for testing and validating application code in a simulation environment [INS22]. One or multiple vehicles can be simulated. To simulate the IoD using Dronekit, several UAV instances can be started, running on different ports. The MAVLink protocol[5] can be used to establish communication between them [Rob]. MAVLink is a lightweight messaging protocol for communicating with UAVs and between onboard drone components [Pro]. An existing master had made code for cooperative UAVs, but this was not open-sourced. We found that Dronekit was unstable when simulating several UAVs, and to overcome this different values for the parameter `SYSID_THISMAV` had to be set for each vehicle. Also, Dronekit only supports Python2.7. Since it was complex to set these parameters and an old Python version was supported, we decided that other programs were more suitable for us.

5.1.4 PX4 with Gazebo and ROS

PX4[6] is an autopilot program that supports SITL. It can be used to connect to Gazebo,[7] a simulation program for robotic environments where one can simulate one or multiple vehicles, like for instance quadcopters, boats, and planes. There are possibilities for connecting PX4 to Robot Operating System (ROS),[8] which is an open-source program that can be of use to build robotic applications. PX4 and the

[2] https://github.com/telematics-lab/IoD_Sim

[3] https://www.nsnam.org/

[4] https://github.com/dronekit/dronekit-python

[5] https://mavlink.io/en/

[6] https://docs.px4.io/main/en/

[7] https://gazebosim.org/home

[8] https://www.ros.org/

core of ROS have a BSD 3-Clause license, which permits private use. ROS is also distributed under permissive open-source licenses like Apache 2.0, and so is Gazebo Classic.

When running PX4 with ROS, ROS nodes are created. A node is a process that performs computation and communicates with other nodes using topics. There can be several nodes to a UAV, one can for example control the rotors and another localization. [ROS18]

PX4 uses MAVLink with UDP to communicate with GCSs by default. It is possible to see and steer the UAVs with for instance QGroundControl.[9] UAVs created by Gazebo with PX4 will appear in this program, and you can create missions for them to perform autonomously and perform other actions. By sending commands using the interface in QGroundControl, one can send a variety of MAVLink messages. It is possible to enable failures in, for example, the GPS or gyroscope, or send fake GPS signals. It is also possible to control the vehicle(s) in offboard mode from a ROS node, where one can send commands to the vehicle [PX423a]. The architecture of the software can be seen in Figure 5.1.

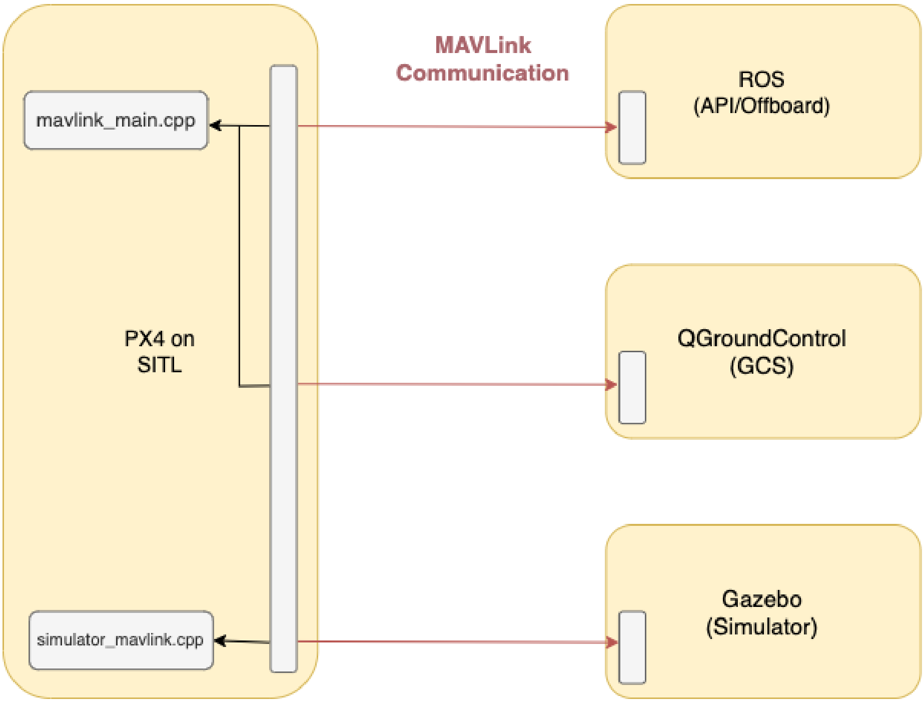


Figure 5.1: Software architecture (inspired from [PX423b])

[9] http://qgroundcontrol.com/

ROS 1 is the original version of ROS. It uses a package called MAVROS to communicate with PX4 over MAVLink. MAVROS is a bridge between ROS 1 topics and the MAVLink protocol. MAVROS can be used for offboard control by publishing MAVROS messages to MAVROS topics.

ROS 2 uses a communications middleware, XRCE-DDS, which can run over different links like UDP and TCP, to communicate with PX4. There is one XRCE-DDS agent and one client that are used to publish and subscribe to topics, which are ROS 2 nodes. It is possible to publish ROS 2 messages to the topics in order to control the vehicle(s) [aut23b], similar to MAVROS in ROS 1. Multiple clients can be connected to the same agent over UDP, enabling multiple vehicle simulation [aut23a].

Table 5.1 summarizes the characteristics of the evaluated software. The requirements for our software were a GUI, the ability to simulate multiple UAVs, open license, that the program was worth using timewise, and that GPS spoofing was feasible. We found that PX4 with Gazebo, both with and without the use of ROS, met our requirements as it offered a convenient approach to generate multiple UAVs connected to a visual GUI. When reading about the software, we noticed several GPS plugins and files and understood that GPS spoofing would be feasible with this software. In the end, this was the chosen software.

	BlueSky	**IoD_sim**	**DroneKit**	**PX4 with Gazebo**	**PX4 with Gazebo and ROS 1/2**
GUI	✓		✓	✓	✓
Multiple UAVs	✓	✓	✓	✓	✓
Communication between UAVs			✓		✓
Open license	✓	✓	✓	✓	✓
Programming language(s)	Python3	C++	Python2.7	C++/Python3	C++/Python3

Table 5.1: Software characteristics

5.2 GPS Spoofing

In this section, several GPS spoofing experiments were performed where the goal was to see how this impacted the UAVs, and to get an idea of how realistic it might be to perform in the real world. The purpose of the attacks involved creating disorientation and taking control of the UAV through the transmission of deceptive GPS signals, with the possibility of directing it towards our intended destination. In this experiment we were only spoofing the GPS signal of one UAV. If this attack was performed in real life, one can assume that if the UAVs flew close to each other, all the UAVs in that area would be affected. However, if they flew kilometers apart and a directional antenna were to be used, one can assume that only one of the UAVs would be spoofed.

First, simulated UAVs were sent out on a mission, creating a swarm. Several missions were performed, and the mission plans were uploaded before takeoff. In these experiments, the UAVs did not communicate with each other during the mission. Fake GPS signals were sent to *one* of the UAV in the swarm.

Second, one UAV was controlled by a running script, called offboard mode, where the UAV was programmed to fly in one direction. Then, a GPS spoofing script was launched that could remotely steer the UAV to a new destination. The fake GPS signals were directed at the specific UAV, and this could also be done in real life. The attacks are explained in detail below.

5.2.1 Experimental setup

PX4 with Gazebo, with and without ROS was the software we ended up using. As Gazebo allowed the creation of multiple UAVs and provided proper visualizations together with QGroundControl, this was preferred over the other software. ROS is only supported on Linux, and since Ubuntu 22.04 is not fully compatible with PX4 yet, Ubuntu 20.04 was used. From the documentation, it seemed like PX4 with Gazebo Classic 11 on a Ubuntu 20.04 was the most stable environment at the time of writing. Therefore, an instance of an Ubuntu 20.04 machine was created in VirtualBox on an Ubuntu 20.04 machine, the newest version to date of the PX4 Autopilot firmware, v 1.14, was downloaded, and Gazebo Classic 11 was installed. The instructions from the PX4 User Guide were followed on how to install the different programs.[10] We had to create a VM because of administrator restrictions on our school's computer lab.

It was possible to simulate multiple UAVs with and without the use of ROS.[11] We decided to test GPS spoofing attacks first without ROS, then ROS 1 and lastly ROS 2.

5.2.2 GPS Spoofing Using MAVLink

The first scenario simulated was a mission consisting of four UAVs in Baylands Park, with a GPS spoofing attack occurring. Multiple UAVs were created by launching an existing script in Gazebo using the command `./Tools/simulation/gazebo-classic/sitl_multiple_run.sh -n` from the PX4-autopilot root package, where *n* specified the number of UAVs. The mission start of the UAV swarm can be seen in Figure 5.2. To the left one can observe the UAVs in the Gazebo simulator, and to the right in QGroundControl. After a while, the UAVs had flown past the first checkpoint, which can be seen in Figure 5.3. Red indicates the path flown, and orange indicates the route that remains. QGroundControl used Vehicle 1, Vehicle 2, etc. to name the UAVs, but in the text, we have called them UAV 1 and UAV 2 and so on.

[10] https://docs.px4.io/main/en/dev_setup/dev_env_linux_ubuntu.html

[11] https://docs.px4.io/main/en/sim_gazebo_classic/multi_vehicle_simulation_gazebo.html

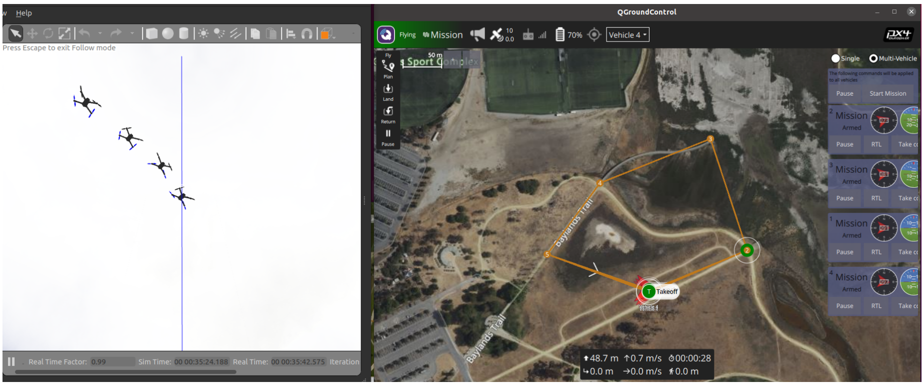


Figure 5.2: UAV swarm

Baylands Park is one of the pre-configured worlds in Gazebo, and hence the UAVs started at that location. The attack was executed using the PX4 fake_gps plugin in the MAVLink terminal, shown in Figure 5.4. The command was started by writing `fake_gps start`. The GPS spoofing is illustrated in Figure 5.5 and it can be seen that UAV 4 has got a different path than the other UAVs.

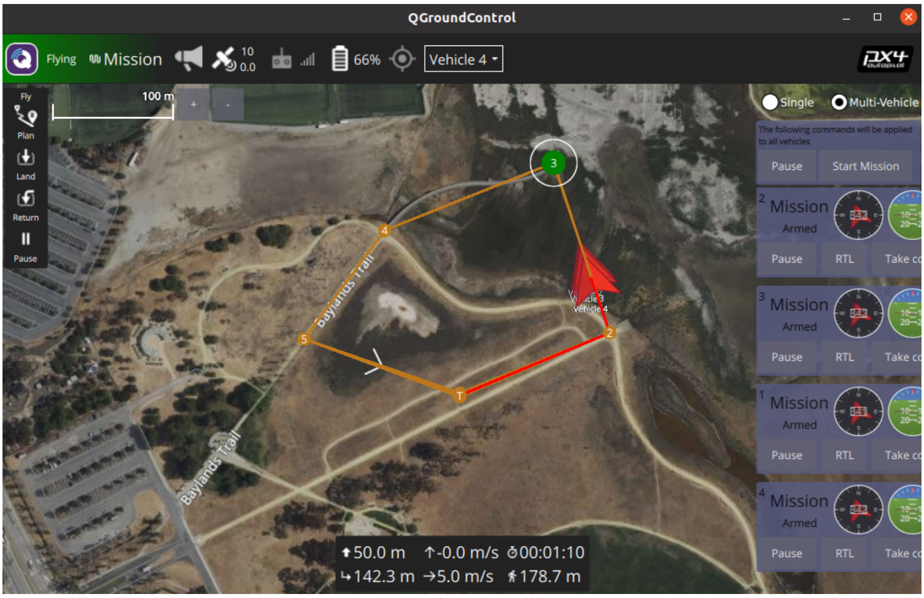
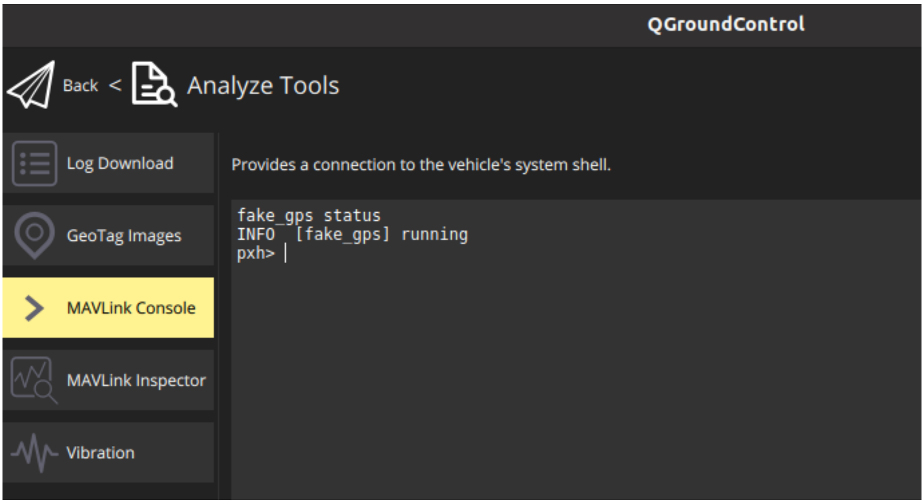


Figure 5.3: Four UAVs performing a mission in Baylands Park



Provides a connection to the vehicle's system shell.

```
fake_gps status
INFO  [fake_gps] running
pxh> |
```

Figure 5.4: Fake GPS running in console

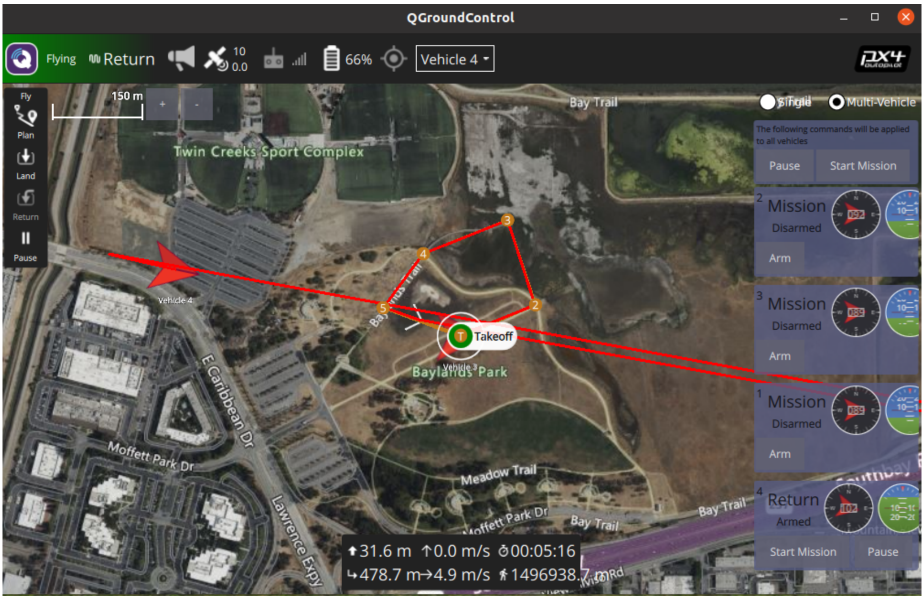


Figure 5.5: GPS spoofing during a mission in Baylands Park

The second scenario simulated was four UAVs on an automated mission in Trondheim, Norway. A mission plan was created and uploaded to each vehicle. The mission plan is attached in Appendix B. By default, the start coordinates were in Baylands Park, so they were changed to make the UAVs start in Trondheim. QGroundControl was used to start the UAVs missions simultaneously. The UAVs performed the pre-defined mission, which can be seen in 5.6. To the left in the Figure, the Gazebo simulator shows the UAVs flying on a line.

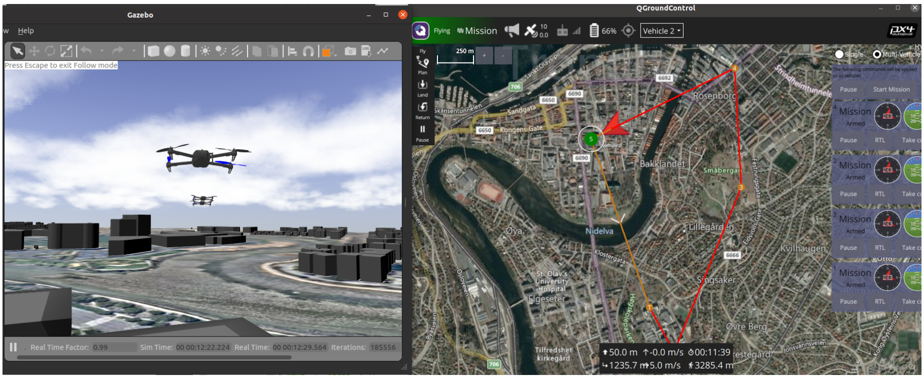


Figure 5.6: Four UAVs performing a mission in Trondheim

GPS spoofing attacks were performed in Trondheim the same way as in the example in Baylands Park, affecting UAV 2. The results can be seen in Figure 5.7.

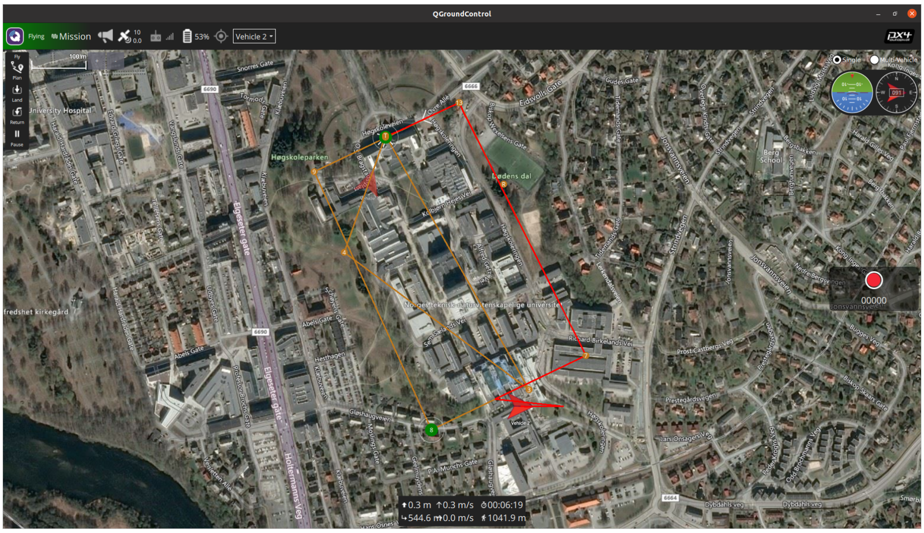


Figure 5.7: GPS spoofing during a mission in Trondheim

5.2.3 GPS Spoofing Using ROS

ROS 1 and MAVROS

A setup with ROS 1, MAVROS, and QGroundControl was used to perform offboard control of one UAV and perform GPS spoofing. In our ROS workspace, we created a ROS package called `offboard_py`. In this package, two Python files were created. The file that programmed the takeoff and path of the UAV was called `offb_node.py`. The other file which performed the spoofing attack to interfere with the pre-programmed path was called `spoofing.py`. In addition, two launch files were created that corresponded to each of the Python scripts. The `start_offb.launch` launched the MAVROS node with SITL and Gazebo, and the node to control the UAV. `spoofing.launch` launched the node that performed the spoofing attack. To launch the attack, we first ran `roslaunch offboard_py start_offb.launch` in one terminal and then we opened a new terminal and ran `roslaunch offboard_py spoofing.launch` when we wanted the spoofing to happen. The ROS files can be found in Appendix C and in our GitHub repository.[12]

The spoofing attack is illustrated in Figure 5.8. In this attack, the UAV was programmed to takeoff to an altitude of 30 meters and then head north-east, 100 meters in the x-direction and 300 meters in the y-direction from the home position (marked with L for “Launch”). After flying for a short period, the spoofing script was launched. The script contained logic that overrode the original course of the UAV and steered the UAV to fly to the GPS coordinates of the SINTEF headquarters (Strindvegen 4, 7034 Trondheim) with a latitude of 63.413808006354735 and a longitude of 10.4111722559795. When the spoofing script was launched, the UAV changed its direction and flew towards “Lerkendal” and SINTEF. This demonstrates a successful hijacking of the UAV, and in a real-world scenario, it could have crashed in the SINTEF office building.

Figure 5.9 shows MAVROS-topics for different UAVs and the corresponding message format. The highlighted topic can be used to set the GPS position.

[12] https://github.com/juliedhj/GPS_spoofing_UAV/tree/master

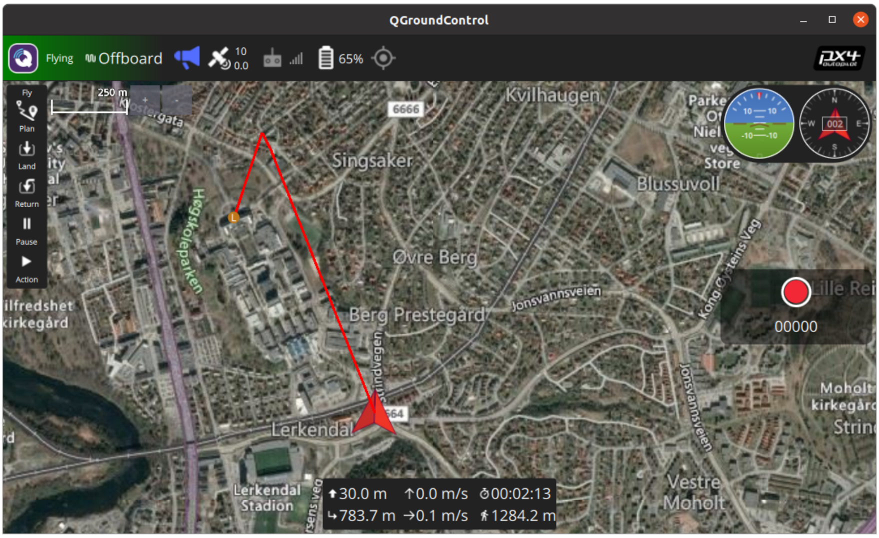
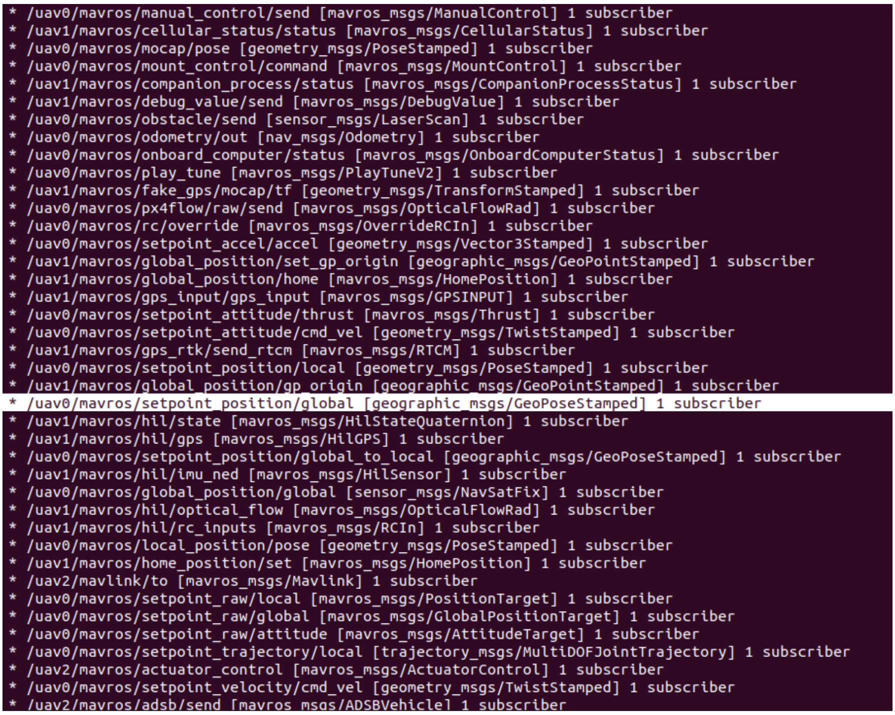


Figure 5.8: Spoofing a UAV using MAVROS

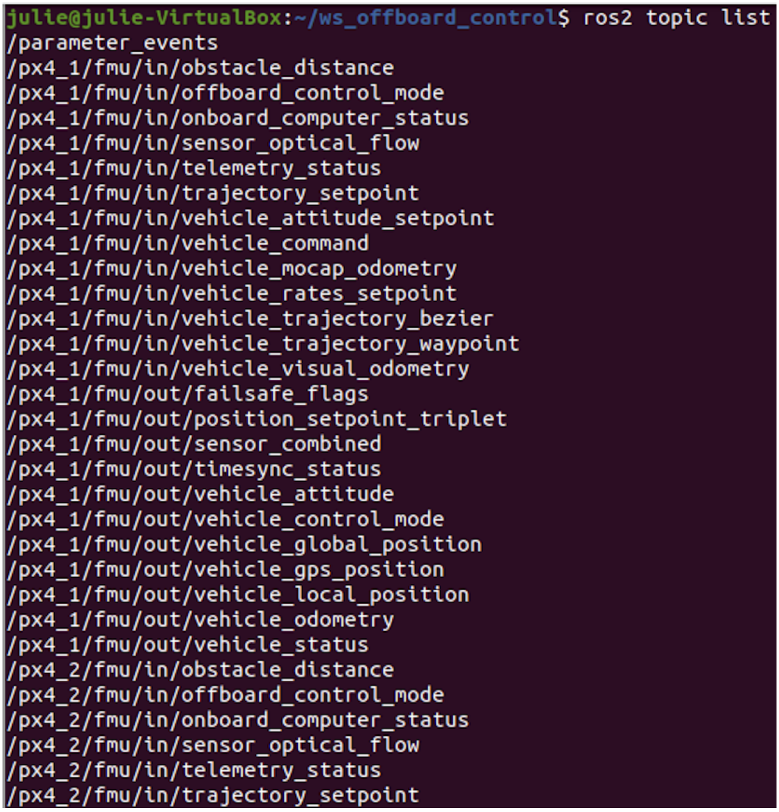


```
* /uav0/mavros/manual_control/send [mavros_msgs/ManualControl] 1 subscriber
* /uav1/mavros/cellular_status/status [mavros_msgs/CellularStatus] 1 subscriber
* /uav0/mavros/mocap/pose [geometry_msgs/PoseStamped] 1 subscriber
* /uav0/mavros/mount_control/command [mavros_msgs/MountControl] 1 subscriber
* /uav1/mavros/companion_process/status [mavros_msgs/CompanionProcessStatus] 1 subscriber
* /uav1/mavros/debug_value/send [mavros_msgs/DebugValue] 1 subscriber
* /uav0/mavros/obstacle/send [sensor_msgs/LaserScan] 1 subscriber
* /uav0/mavros/odometry/out [nav_msgs/Odometry] 1 subscriber
* /uav0/mavros/onboard_computer/status [mavros_msgs/OnboardComputerStatus] 1 subscriber
* /uav0/mavros/play_tune [mavros_msgs/PlayTuneV2] 1 subscriber
* /uav1/mavros/fake_gps/mocap/tf [geometry_msgs/TransformStamped] 1 subscriber
* /uav0/mavros/px4flow/raw/send [mavros_msgs/OpticalFlowRad] 1 subscriber
* /uav0/mavros/rc/override [mavros_msgs/OverrideRCIn] 1 subscriber
* /uav0/mavros/setpoint_accel/accel [geometry_msgs/Vector3Stamped] 1 subscriber
* /uav1/mavros/global_position/set_gp_origin [geographic_msgs/GeoPointStamped] 1 subscriber
* /uav1/mavros/global_position/home [mavros_msgs/HomePosition] 1 subscriber
* /uav1/mavros/gps_input/gps_input [mavros_msgs/GPSINPUT] 1 subscriber
* /uav0/mavros/setpoint_attitude/thrust [mavros_msgs/Thrust] 1 subscriber
* /uav0/mavros/setpoint_attitude/cmd_vel [geometry_msgs/TwistStamped] 1 subscriber
* /uav1/mavros/gps_rtk/send_rtcm [mavros_msgs/RTCM] 1 subscriber
* /uav0/mavros/setpoint_position/local [geometry_msgs/PoseStamped] 1 subscriber
* /uav1/mavros/global_position/gp_origin [geographic_msgs/GeoPointStamped] 1 subscriber
* /uav0/mavros/setpoint_position/global [geographic_msgs/GeoPoseStamped] 1 subscriber
* /uav1/mavros/hil/state [mavros_msgs/HilStateQuaternion] 1 subscriber
* /uav1/mavros/hil/gps [mavros_msgs/HilGPS] 1 subscriber
* /uav0/mavros/setpoint_position/global_to_local [geographic_msgs/GeoPoseStamped] 1 subscriber
* /uav1/mavros/hil/imu_ned [mavros_msgs/HilSensor] 1 subscriber
* /uav0/mavros/global_position/global [sensor_msgs/NavSatFix] 1 subscriber
* /uav1/mavros/hil/optical_flow [mavros_msgs/OpticalFlowRad] 1 subscriber
* /uav1/mavros/hil/rc_inputs [mavros_msgs/RCIn] 1 subscriber
* /uav0/mavros/local_position/pose [geometry_msgs/PoseStamped] 1 subscriber
* /uav1/mavros/home_position/set [mavros_msgs/HomePosition] 1 subscriber
* /uav2/mavlink/to [mavros_msgs/Mavlink] 1 subscriber
* /uav0/mavros/setpoint_raw/local [mavros_msgs/PositionTarget] 1 subscriber
* /uav0/mavros/setpoint_raw/global [mavros_msgs/GlobalPositionTarget] 1 subscriber
* /uav0/mavros/setpoint_raw/attitude [mavros_msgs/AttitudeTarget] 1 subscriber
* /uav0/mavros/setpoint_trajectory/local [trajectory_msgs/MultiDOFJointTrajectory] 1 subscriber
* /uav2/mavros/actuator_control [mavros_msgs/ActuatorControl] 1 subscriber
* /uav0/mavros/setpoint_velocity/cmd_vel [geometry_msgs/TwistStamped] 1 subscriber
* /uav2/mavros/adsb/send [mavros_msgs/ADSBVehicle] 1 subscriber
```

Figure 5.9: MAVROS topics

ROS 2

For ROS 2, a new instance of Ubuntu 20.04 was created in VirtualBox to ensure that the software would not collide with the ROS 1 setup. The required software was installed, PX4 and the XRCE-DDS Agent were run, and the script for creating multiple UAVs was launched using the command in Section 5.2.2. All ROS 2 topics for the different UAVs could be seen by typing `ros2 topic list` in another terminal. Some topics can be seen in Figure 5.10. Topics that begin with `/px4_1/` define the topics for UAV1 and `/px4_2/` for UAV2, because `sitl_multiple_run.sh` launched a process of PX4 for each UAV. */in* refers to the UAV's subscription topics, and */out* to publishing topics.



```
julie@julie-VirtualBox:~/ws_offboard_control$ ros2 topic list
/parameter_events
/px4_1/fmu/in/obstacle_distance
/px4_1/fmu/in/offboard_control_mode
/px4_1/fmu/in/onboard_computer_status
/px4_1/fmu/in/sensor_optical_flow
/px4_1/fmu/in/telemetry_status
/px4_1/fmu/in/trajectory_setpoint
/px4_1/fmu/in/vehicle_attitude_setpoint
/px4_1/fmu/in/vehicle_command
/px4_1/fmu/in/vehicle_mocap_odometry
/px4_1/fmu/in/vehicle_rates_setpoint
/px4_1/fmu/in/vehicle_trajectory_bezier
/px4_1/fmu/in/vehicle_trajectory_waypoint
/px4_1/fmu/in/vehicle_visual_odometry
/px4_1/fmu/out/failsafe_flags
/px4_1/fmu/out/position_setpoint_triplet
/px4_1/fmu/out/sensor_combined
/px4_1/fmu/out/timesync_status
/px4_1/fmu/out/vehicle_attitude
/px4_1/fmu/out/vehicle_control_mode
/px4_1/fmu/out/vehicle_global_position
/px4_1/fmu/out/vehicle_gps_position
/px4_1/fmu/out/vehicle_local_position
/px4_1/fmu/out/vehicle_odometry
/px4_1/fmu/out/vehicle_status
/px4_2/fmu/in/obstacle_distance
/px4_2/fmu/in/offboard_control_mode
/px4_2/fmu/in/onboard_computer_status
/px4_2/fmu/in/sensor_optical_flow
/px4_2/fmu/in/telemetry_status
/px4_2/fmu/in/trajectory_setpoint
```

Figure 5.10: ROS 2 topics

For the GPS spoofing, we tried creating a spoofing script that published fake GPS signals to the relevant topics. We used our knowledge from ROS 1, several forum threads, and the existing scripts in the ROS 2 workspace for this. Unfortunately, due to time limitations and differences between the two ROS versions, ROS 2 was tried out, but we did not succeed in performing any spoofing attacks with this software. This was mainly due to the lack of documentation for using Python in ROS 2. The documentation contained a C++ and Python example for controlling the UAV using ROS 2, but it only documented how to use the C++ example. To run Python code, some additional support for Python had to be implemented.

Chapter 6

Resource Cost Modeling

This chapter models the resource cost according to the methodology described in Chapter 2. This presents an understanding of what resources are necessary to carry out the chosen attacks and the associated cost. Two attacks were chosen based on our findings in the literature studies and interviews. These are GPS spoofing and DoS. The RCM has been used to estimate the cost of GPS spoofing before, but never in the context of UAVs.

When it comes to estimating the cost intervals based on the time and effort needed, we assume that one hour is worth \$20. This is, for example, the case when the attacker has the option to produce scripts or modify existing scripts. The cost interval is also dependent on the attacker's skills in these cases; the more skilled he is, the less time it will take. Moreover, there exist resources on other sites than those we found that will work for the attacks as well, which may have higher or lower prices than the ones found. Therefore, the confidence values are set to 0.8 in such cases. In the analysis, we assume that the attacker already owns a computer that can be used in the attacks. For that reason, it is not included as a resource in any of the resource trees.

6.1 Cost Estimation of GPS Spoofing

GPS spoofing is a prominent threat to UAVs and IoD. This section will look at the necessary resources needed to perform a GPS spoofing attack on a single UAV, and the associated cost. The starting point of the GPS spoofing is a similar analysis done by Haga [Hag20] and Walde & Hanus [WH20].

6.1.1 Reconnaissance

At the reconnaissance stage, the adversary must select a victim UAV and acquire the resources in Figure 6.1. Primarily, one needs to find the location of the UAV. This can be done either by observing a UAV in the air or by using tracking systems or apps. DJI has developed a drone detection unit[1] which can be used to track DJI UAVs. There are also other drone detection systems on the market. To find the price of these drone detection systems, one would need to contact the developers to get an offer. We contacted DJI to get a price for their drone detection unit, and the minimum price starts at $2000 for one year. The other alternative, apps, could for instance be DroneWatcher or AirMap [Kar22], which can be downloaded for free.

The next step is to understand how GPS communication and signal processing work to be able to create a fake signal. Information on this can be found publicly on the Internet.

To estimate the coverage of the attack, meaning how close you must be in order to execute the spoofing attack, it would be ideal to test this on a physical UAV as this would be very accurate. However, since this has not been possible for us to do, we found it difficult to estimate the related cost. It is also essential to consider the terrain, and if the area is populated, which will affect the coverage of the attack. Theoretical calculation of the coverage requires knowledge we do not possess; therefore, the cost of this resource alternative is hard to determine. Another solution to test the coverage could be to use open-source software, like, for example, RF Range Calculator[2] developed by Silicon Labs.

[1] https://www.dedrone.com/solutions/dedrone-rapid-response

[2] https://community.silabs.com/s/article/rf-range-calculator?language=en_US

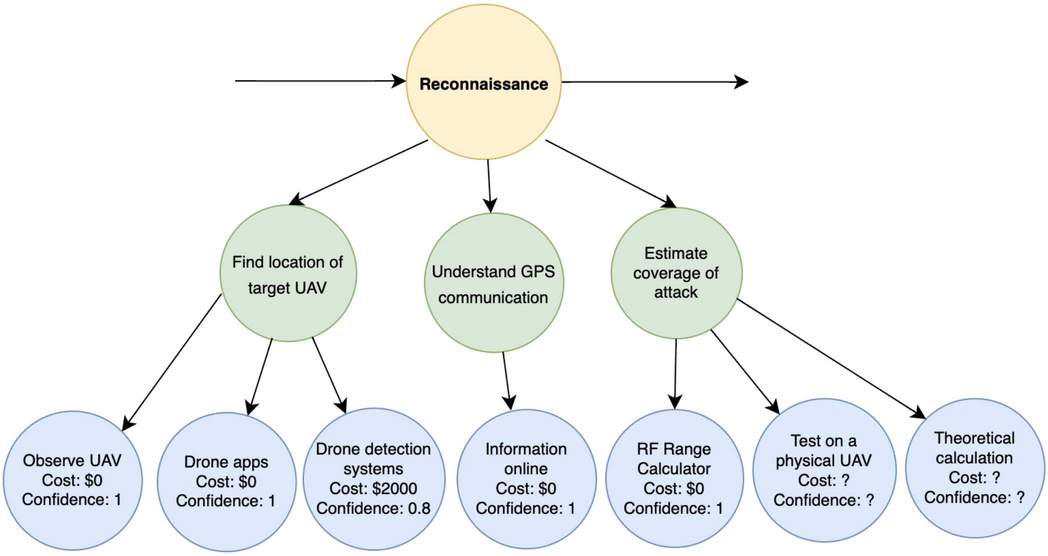

Reconnaissance
Find location of target UAV
Understand GPS communication
Estimate coverage of attack
Observe UAV Cost: $0 Confidence: 1
Drone apps Cost: $0 Confidence: 1
Drone detection systems Cost: $2000 Confidence: 0.8
Information online Cost: $0 Confidence: 1
RF Range Calculator Cost: $0 Confidence: 1
Test on a physical UAV Cost: ? Confidence: ?
Theoretical calculation Cost: ? Confidence: ?

Figure 6.1: GPS spoofing: Reconnaissance

6.1.2 Weaponization

To spoof the GPS, one can use GPS signal simulators. They emit fake GPS signals that can make a UAV deviate from its intended course. There are many open-source tools available for this purpose, like for instance `GPS-SDR-SIM`[3] and `Multi-sdr-gps-sim`[4] that can be used together with a Software Defined Radio (SDR). We assume some modifications are needed to adapt the software to the use case and therefore estimate that this would have an associated cost ranging from $200 to $2000, which is between 10 and 100 hours of work. A quick Google search indicates that the prices of SDRs range from $100 to $1500 depending on the vendor, giving a total minimum of $300 and a maximum of $3500. It is also possible to use physical hardware GPS simulators, and the prices range from $183 to $29 500.[5] Lastly, one can create a script. The cost based on time and effort would range from $100 to $5000, and an SDR is also needed, resulting in a total cost range from $200 to $6500, and lower confidence of 0.6 because of uncertainties related to the time it will take. We have taken the time of our GPS spoofing experiments into account when deciding the maximum amount. The weaponization stage is illustrated in Figure 6.2.

[3] https://github.com/osqzss/gps-sdr-sim

[4] https://github.com/Mictronics/multi-sdr-gps-sim

[5] https://www.alibaba.com/trade/search?fsb=y&IndexArea=product_en&keywords=gps+simulator&viewtype=G&&pricef=&pricet=

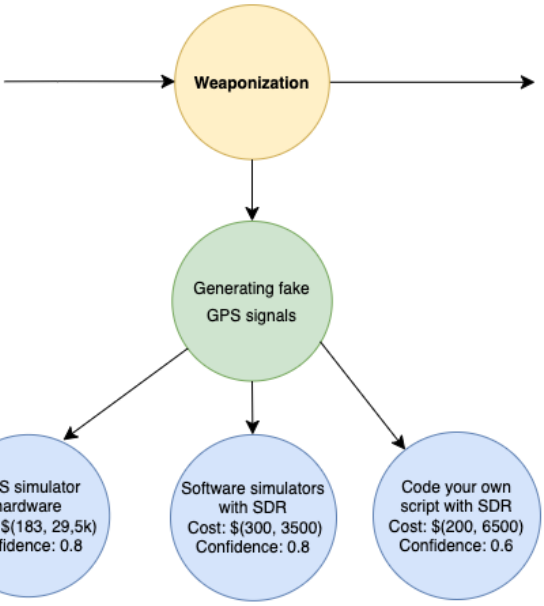

Weaponization
Generating fake GPS signals
GPS simulator hardware Cost: $(183, 29,5k) Confidence: 0.8
Software simulators with SDR Cost: $(300, 3500) Confidence: 0.8
Code your own script with SDR Cost: $(200, 6500) Confidence: 0.6

Figure 6.2: GPS spoofing: Weaponization

6.1.3 Delivery

At the delivery stage, the attacker transmits the fake GPS signals to the receiving antenna. To achieve this, the victim UAV must be forced to perform a signal re-acquisition. There are three resources required for this. Firstly, jamming is required to force the target to search for new signals and hence pick up the wrong GPS signals [Hag20]. Jamming can be introduced by using a drone gun jammer, a portable jammer, or a stationary jammer. They can range in prices from $50 to $22 000. [6,7,8]

Next, the attacker needs to ensure he has a radio transmitter near the target. This can be achieved through RADAR or laser-based rangefinders. The price range from RADAR is estimated to be $49 to $826,[9,10] and the price range for laser-based rangefinders is $17 to $2821.[11]

[6] https://www.zdnet.com/article/cheap-gps-jammers-endanger-drones/

[7] https://jammers4u.com/drones-jammer?sort=p.price&order=ASC

[8] https://www.perfectjammer.com/drone-signal-jammers.html

[9] https://www.dedetoshop.com/?category_id=697288

[10] https://www.proshop.no/Droner/DJI-CSM-Radar-for-M300/2957188

[11] https://www.ebay.com/sch/i.html?_from=R40&_nkw=laser+rangefinders&_sacat=0&_sop=12

Furthermore, the GPS signals need to be sent at a greater strength that overrides the original data [Hag20]. This can be done by using a signal booster with a price from $725 to $3200.[12] The delivery stage is illustrated in Figure 6.3.

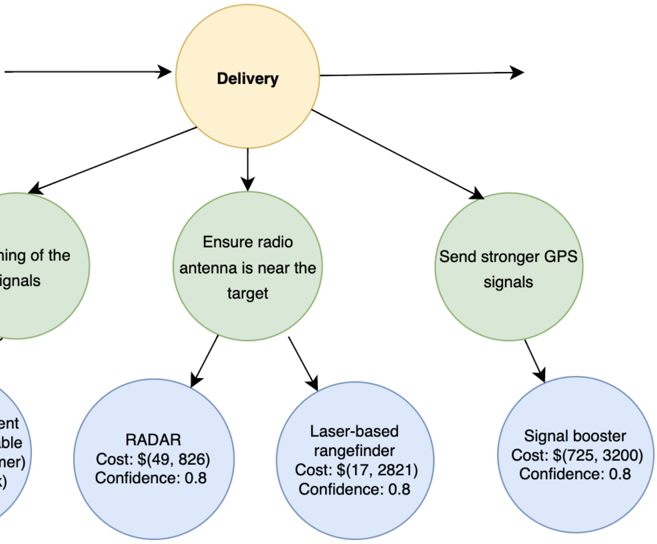


Figure 6.3: GPS spoofing: Delivery

6.1.4 Exploitation

As mentioned in Chapter 3, civilian GPS signals are unencrypted and unauthenticated. This is something an adversary can take advantage of in the exploitation stage. No resource alternatives are needed at this stage, as this is an underlying problem with the system itself. The exploitation stage is illustrated in Figure 6.4.

[12] https://mysignalboosters.com/nz/shop/

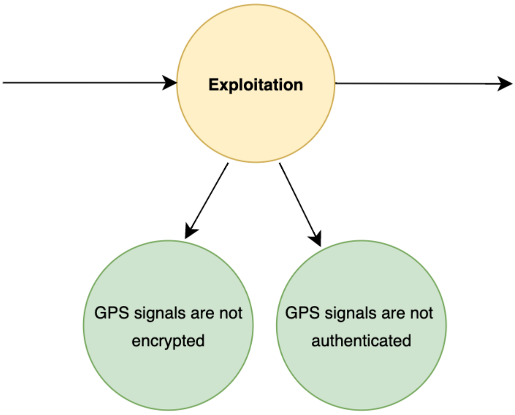

Exploitation
GPS signals are not encrypted
GPS signals are not authenticated

Figure 6.4: GPS spoofing: Exploitation

6.1.5 Installation

At the installation stage, the target processes the spoofed GPS signals. The resources needed to accomplish the installation stage include a SDR, a RF generator, and a radio transmitter. The SDR is required to transform the fake signals into radio frequencies. Further, the RF generator generates the actual signals, before the radio transmitter sends these to the UAV [Hag20]. See Figure 6.5 for the resource tree.

The SDR could be a HackRF One to $340,[13] but since we already have acquired a SDR in the weaponization stage, the cost will be $0. The antenna ANT 500 can be used as both a radio transmitter and receiver. It is designed to fit the HackRF one and can be bought for $35.[14] The cost range of a RF generator varies a lot. Some cost a few hundred dollars, and others cost as much as $20 000.[15]

[13] https://www.adafruit.com/product/3583

[14] https://www.amazon.com/ANT500-Telescopic-Antenna-HackRF-Stick/dp/B01CQYZJV2

[15] https://no.rs-online.com/web/c/test-measurement/signal-generators-analysers/rf-signal-generators/?pn=1&rpp=100

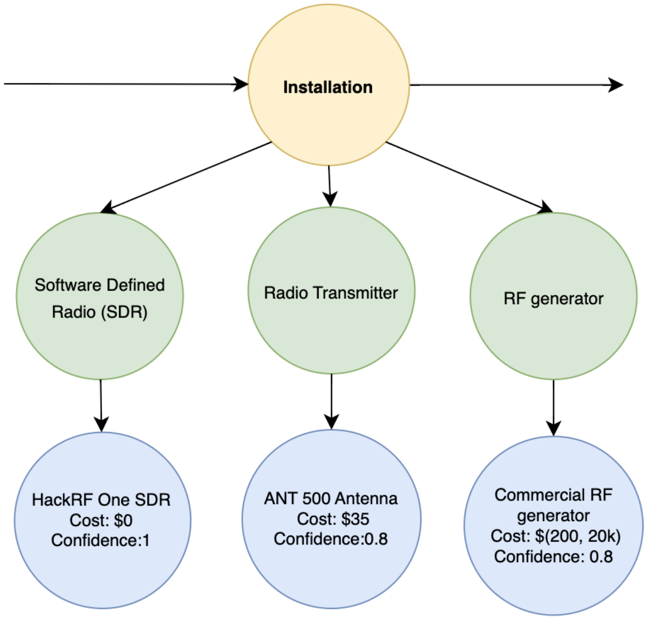


Figure 6.5: GPS spoofing: Installation

6.1.6 Command & Control

To maintain control over the target UAV in a GPS spoofing attack, the adversary needs to continuously transmit the fake GPS signals [Hag20]. To do this, the adversary needs to know the position of the UAV, so it can be within the range of the transmitter. This can be done by for example pursuing the UAV, for example, by car, motorcycle, or with another UAV. The price of a suitable UAV can range from $50 to $2450.[16] For the other vehicles, we make a rough estimation of a price range between $500 and $5000. There are more expensive ones, but we assume that they are not necessary to achieve the objective. There will be some additional costs for fuel and a driver so the confidence for this will be 0.8. The stage is illustrated in Figure 6.6.

[16] https://www.elkjop.no/sport-hobby-og-fritid/droner-og-tilbehor/drone

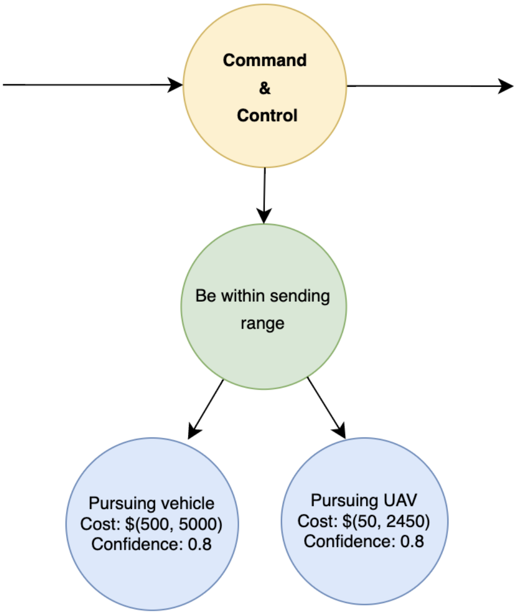


Figure 6.6: GPS spoofing: Command & Control

6.1.7 Actions on Objective

At the final stage, the adversary aims to fulfill his original goal, which was to spoof the victim UAV to another location or make it deviate from its intended course. General knowledge of the flight plan should be known to the adversary. This way he can be careful not to make a too rapid change in the direction, as this would probably be detected. Such information can be obtained using several applications. For DJI UAVs, there is an application called Drone Scanner that provides an overview of UAVs near you, including their altitude, location, and direction.[17] Drone detection systems may also be used to espionage on the drone to figure out approximately where it is headed. No additional resource alternatives are necessary at this stage.

[17] https://dronedj.com/2022/10/04/remote-id-drone-tracking-app/

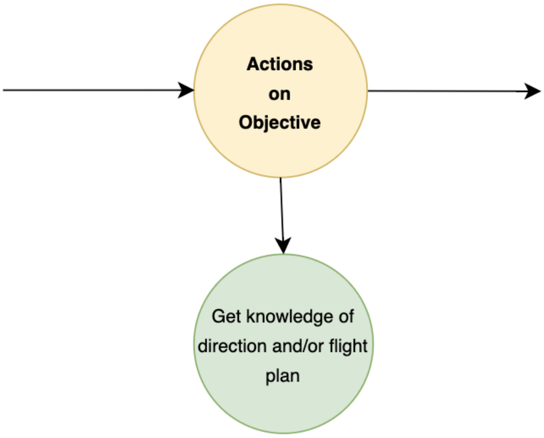


Figure 6.7: GPS spoofing: Actions on Objective

6.1.8 Estimation of Total Cost

The RCM presents resources needed to conduct and succeed in GPS spoofing a UAV. Some of the resources required were a SDR, a jammer, and fundamental knowledge of GPS communication. The resource alternatives varied among different types of jammers, SDRs, and online resources. The costs related to the resource alternatives were found and used for the cost estimation below.

To calculate the cost estimates of GPS spoofing a UAV, the minimum cost for each stage was found by summarizing the cheapest resource alternative needed to realize each resource, according to the description in Chapter 2. The same calculation was applied to the most expensive resource alternatives. Summarizing the minimum and maximum costs of each stage gave the total minimum and maximum cost estimations. For the confidence value of a stage, the average confidence to realize each resource was calculated and multiplied. Total confidence was found by taking the product of the confidence of each stage. The costs for each stage are summarized in Table 6.1.

Using the equations discussed in Chapter 2, we get the following numbers:

Equation 2.2 derives the sum of minimum costs, which is \$1260
Equation 2.3 derives the sum of maximum costs, which is \$84 556
Equation 2.5 derives the product of the confidence values, which is 0.224

CKC stage	Min cost	Max cost	Confidence
Reconnaissance	$0	$2000	0.933
Weaponization	$183	$29 500	0.733
Delivery	$792	$28 021	0.64
Exploitation	$0	$0	1
Installation	$235	$20 035	0.64
Command & Control	$50	$5000	0.8
Actions on Objectives	$0	$0	1
Total	**$1260**	**$84 556**	**0.224**

Table 6.1: Cost estimations of GPS spoofing a UAV

From the results, it is apparent that there is a relatively low minimum cost associated with GPS spoofing a UAV based on the resource alternatives found. Also, the maximum cost is much greater, at approximately $85 000. The confidence related to these costs is, however, a bit low at 0.224. The stages that influence confidence the most are delivery and installation, both with confidence values of 0.64. Both these stages require a few resources, which have some uncertainties related to the cost intervals of the resource alternatives.

6.2 Cost Estimation of Denial of Service

Another common threat facing UAVs and IoD is DoS attacks, which was mentioned in literature and the interviews. Therefore, the second attack with cost and resource estimation is DoS attacks. In this scenario, an assumption is that the GCS and UAV communicates using WiFi and use private IP addresses. We want to address flooding of requests to the IP address belonging to the target, namely the UAV or the GCS.

6.2.1 Reconnaissance

To be able to carry out a DoS attack, the adversary needs to have knowledge about how DoS attacks work and how UAVs communicate. This can be learned from online available sources.

To discover the network the UAV operates on, it is not sufficient to use the network card on a computer because of its short range. Therefore, an antenna can be used to enhance the signals. Antennas come in different price ranges, from $10 to

$86 for more advanced antennas.[18,19]

To further locate the exact network that is used by the UAV and GCS, `Wireshark`[20] can be used to dump the traffic. For many UAVs, the network will have a name that reflects the product type, like for instance "PHANTOM3_XXXXXX" for DJI's PHANTOM3 [DJI15], and "ardrone_XYXYXYXYXYXY" for Parrot's AR.Drone [Par]. Therefore, the adversary can assume he has the correct network if similar names appear.

To obtain the IP address of the entities, a connection to the network is needed. The adversary can connect to the network if it is an open network, meaning it has no security features. On the other hand, if the network is password protected, one can use tools like `Aircrack-ng`[21] and `John the Ripper`[22] on the traffic dump. These tools are available for free online. Many DJI UAVs have the default password "12341234" [DJI15], which can be found quickly using these tools. It is not unreasonable to assume that other vendors also use default passwords. Statistics show that 35% of people never change their passwords,[23] and leaving the UAV with a default password makes it somewhat feasible to crack the password. The time it will take to crack the password is dependent on the password length, if it is a common word, and if numbers and symbols are used. We estimate that cracking it can take a few hours up to several days, resulting in a cost interval of $40 to $3360. We here chose two hours up to a week, with a confidence of 0.6 since these are guesses on our part. The IP address of the UAV or GCS can be obtained by `Wireshark` or by guessing it.

In addition, the adversary must find out which ports and services are open at the target, to know where to direct the traffic. This will help differentiate between the GCS and the UAV because usually, a UAV has some additional services like for example a video streaming application [MVC+16]. An alternative tool for this purpose is `Network Mapper (Nmap)`,[24] which is an open-source tool for network discovery and security auditing.

Many of the resource alternatives for this stage do not require a substantial amount of time and effort spent, which is why we have not considered any costs for this.

[18] https://www.amazon.com/Alfa-ARS-N19-OMNI-Directional-High-Gain-Adapters/dp/B009H028CM

[19] https://www.amazon.in/Antenna-World-G2424-Directional-Parabolic/dp/B00NQGVMSE

[20] https://www.wireshark.org/

[21] https://www.aircrack-ng.org/

[22] https://www.openwall.com/john/

[23] https://uk.pcmag.com/password-managers/116459/35-percent-of-people-never-change-their-passwords

[24] https://nmap.org/

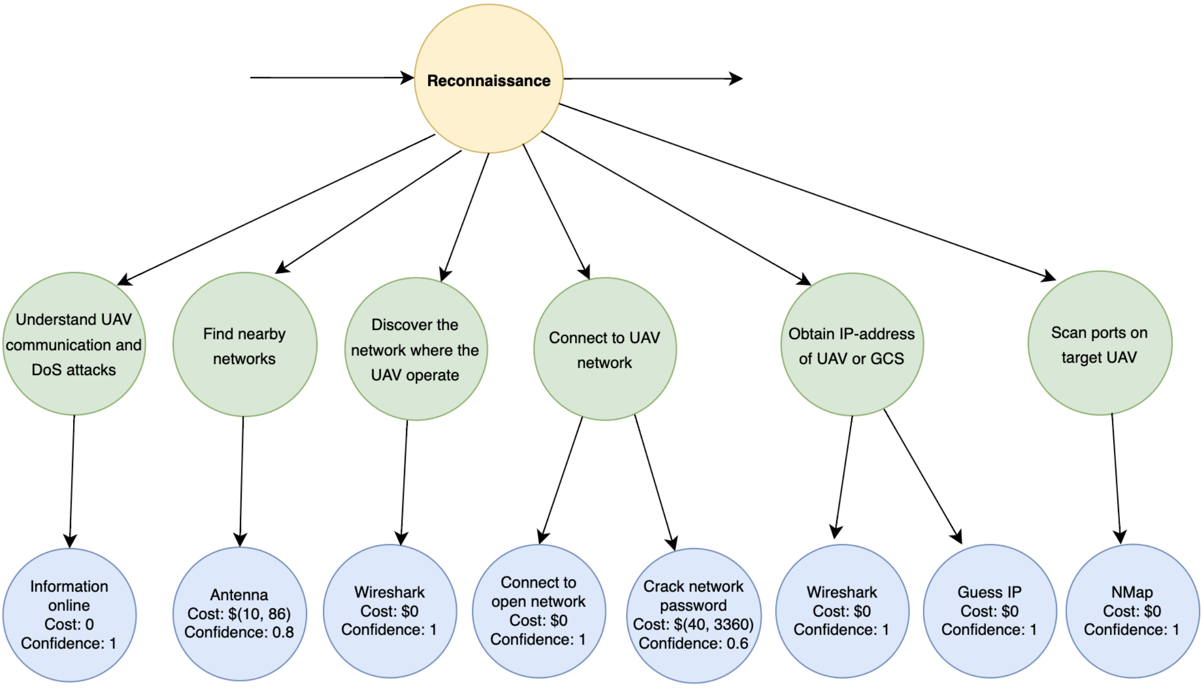


Figure 6.8: DoS: Reconnaissance

6.2.2 Weaponization

This stage involves configuring attack scripts and preparing exploit payloads. There are free packet generator applications that can easily create data packets to send to the UAV's network [HCA+21a]. They are also called network stress testing tools. Some packet generator tools are `hping`[25] and `Low Orbit Ion Cannon (LOIC)`.[26]

Some additional effort may be necessary to get the code working, so we estimate that this has a cost ranging between $20 to $800 corresponding to between 1 and 40 hours, with a confidence of 0.8. The cost is dependent on how many modifications to the code are needed, and the attacker's skills. For instance, if `hping` were to be used, we assume it would be straightforward. The weaponization stage is illustrated in Figure 6.9.

[25] http://wiki.hping.org/

[26] https://github.com/NewEraCracker/LOIC

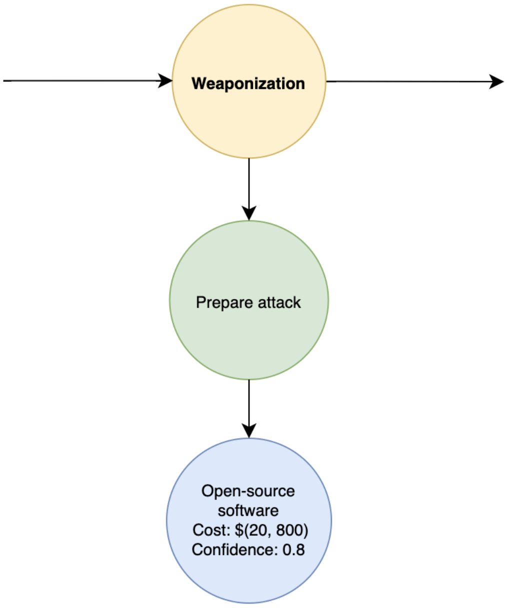


Figure 6.9: DoS: Weaponization

6.2.3 Delivery

At the delivery stage, the attacker delivers the traffic to the target UAV or GCS to congest the network. It can be performed by having obtained the IP address and using some of the tools mentioned in the weaponization stage, where only the target IP address is required. No further resource alternatives are needed at this stage. The delivery stage is illustrated in Figure 6.10.

6.2.4 Exploitation

The target UAV needs to be vulnerable to a DoS attack by not having proper mitigations for detecting and stopping DoS attacks. Wireless communication is known to be vulnerable to a variety of attacks, and since UAVs use wireless communication, this makes them vulnerable. In addition, the exploit is possible if the WiFi settings are poor, for example, having an open network, using weak WiFi protocols, or easy-to-guess passwords, which enables the attacker to access the network and hence obtain the IP address. The exploitation stage is illustrated in Figure 6.11.

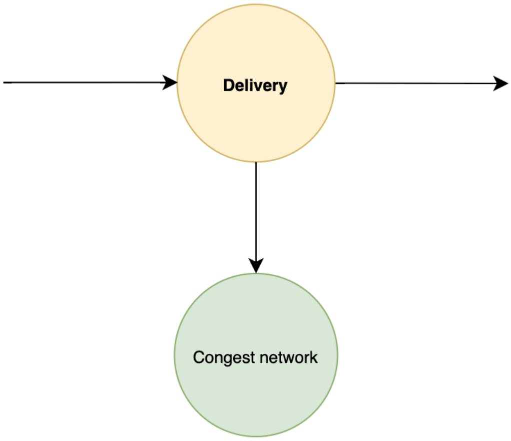


Figure 6.10: DoS: Delivery

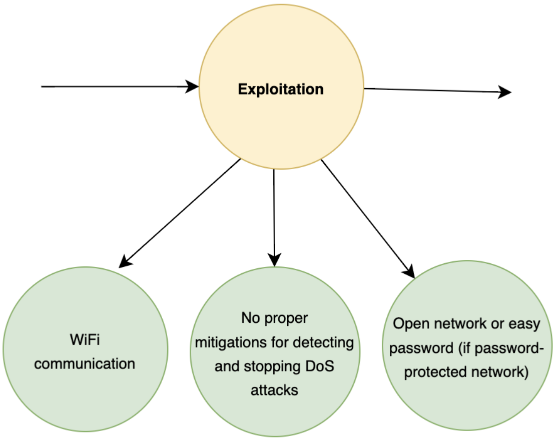

Exploitation
WiFi communication
No proper mitigations for detecting and stopping DoS attacks
Open network or easy password (if password-protected network)

Figure 6.11: DoS: Exploitation

6.2.5 Command & Control

During the DoS attack, the adversary continuously transmits traffic to the target. As stated before, he needs to stay connected to the same network as the UAV and GCS. This can be done by pursuing it, in the same ways mentioned in the RCM GPS spoofing. See Figure 6.12 for this stage.

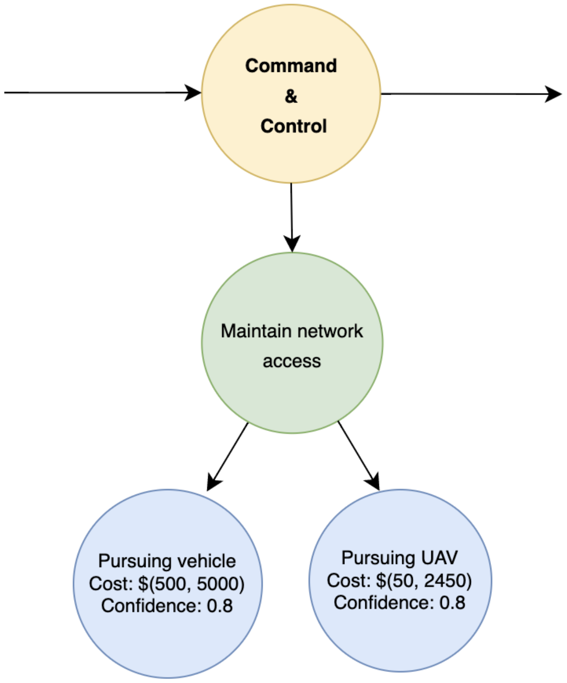


Figure 6.12: DoS: Command & Control

6.2.6 Actions on Objective

Here, the adversary completes his original goal, which was to make the UAV unavailable and hopefully make it crash. After some time receiving a lot of traffic, the server stops responding to legitimate requests from the GCS. If no fail-safe actions are activated, it would most likely crash and the attacker would violate the availability. Examples of fail-safe actions could include automatically returning the UAV to its home base or reducing its speed if the UAV encounter any unexpected issues [TS223]. There are no relevant resources needed at this stage.

6.2.7 Estimation of Total Cost

In this section, the prerequisites for successfully carrying out a DoS attack to a UAV were found. From the modeling, a key point is that obtaining and maintaining access to the network used by the GCS and UAV is important for the adversary. He also needs to have some knowledge of how to find the password of a WiFi network and the tools used for this. The total cost is calculated the same way as the cost on GPS spoofing. The cost for each stage is summarized in Table 6.2.

CKC stage	**Min cost**	**Max cost**	**Confidence**
Reconnaissance	$50	$3446	0.64
Weaponization	$20	$800	0.8
Delivery	$0	$0	1
Exploitation	$0	$0	1
Installation	N/A	N/A	N/A
Command & Control	$50	$5000	0.8
Actions on Objectives	$0	$0	1
Total	**$130**	**$9246**	**0.41**

Table 6.2: Cost estimations of a DoS attack against a UAV

Using the equations discussed in Chapter 2, we get the following:

Equation 2.2 derives the sum of minimum costs, which is $130
Equation 2.3 derives the sum of maximum costs, which is $9246
Equation 2.5 derives the product of the confidence values, which is 0.41

The cost estimation of the DoS attack resulted in a minimum cost of $130, which is a low cost. However, the maximum cost is greater, at approximately $9250. The confidence is relatively high at 0.41. The reconnaissance stage influences the confidence value the most because it requires a lot of resources. However, most of them can be acquired for free, so the costs are not too significant at this stage.

Chapter 7 Analysis of Cybersecurity Threats

This chapter aims to identify the cybersecurity threats associated with the IoD as a part of our results. It contains threats specific to the IoD architectures, to an IoD network, and a table summarizing all the threats related to UAVs and IoD. By exploring these threats, we gain insight into vulnerable components and what cybersecurity attributes are violated. The threats presented in this chapter are gathered from the literature studies and the interviews.

Figure 7.1 presents threats to the three IoD architectures presented in Figure 3.3 in Chapter 3. While these architectures provide numerous benefits, they also face various threats and vulnerabilities. The architectures contain potentially vulnerable elements exposed to attacks which are marked in red and further discussed.

In the IoD architecture based on the cloud, an adversary could get access to the cloud by, for example, exploiting a password or succeeding in a phishing attack. In general, employing on-premise servers offers greater security, while the cloud presents a more cost-effective solution. Cloud-based IoD architecture may be vulnerable to DoS attacks, where an attacker overwhelms the cloud infrastructure with a flood of requests, causing service disruption. However, using a well-known cloud service provider like for instance Azure,[1] Amazon Web Services (AWS),[2] or the Google Cloud Platform (GCP)[3] will limit the chances of DoS attacks. Furthermore, the UAV at the drone layer could be malicious and send false data.

For the IoT-based IoD architecture, the link between the flying zone and the GCS could be compromised. The GCS could also be the target of an attack, both physical attacks and attacks targeting the data it receives from the UAVs. The centralized GSS becomes a single point of failure, making the entire system vulnerable to attacks or disruptions. A successful attack on the GSS can lead to losing control

[1] https://azure.microsoft.com/

[2] https://aws.amazon.com/

[3] https://cloud.google.com/

over the UAVs, compromising their operation and potentially causing safety risks. It is also a potential scenario that one or more malicious UAVs in the flying zone could disrupt operations and communication, or gain unauthorized access to the IoD system. Furthermore, the link from the control room could be intercepted and instructions to the UAV could be modified if no proper mitigations are in place.

In the Internet-based IoD architecture, the server is connected to the Internet and is vulnerable to malware and distributed DoS attacks. Malicious code can be injected into the system or a large number of compromised devices can overwhelm the server causing service disruptions. Furthermore, the data link from the Internet could, for instance, be malicious or eavesdropped. The same can happen for the link from the control room. The external user connecting to the Internet can also be an adversary. Storing sensitive data, such as flight plans or live video in a centralized server like in this architecture, increases the risk of data breaches. Malicious actors may attempt to intercept or manipulate the data, compromising privacy and security.

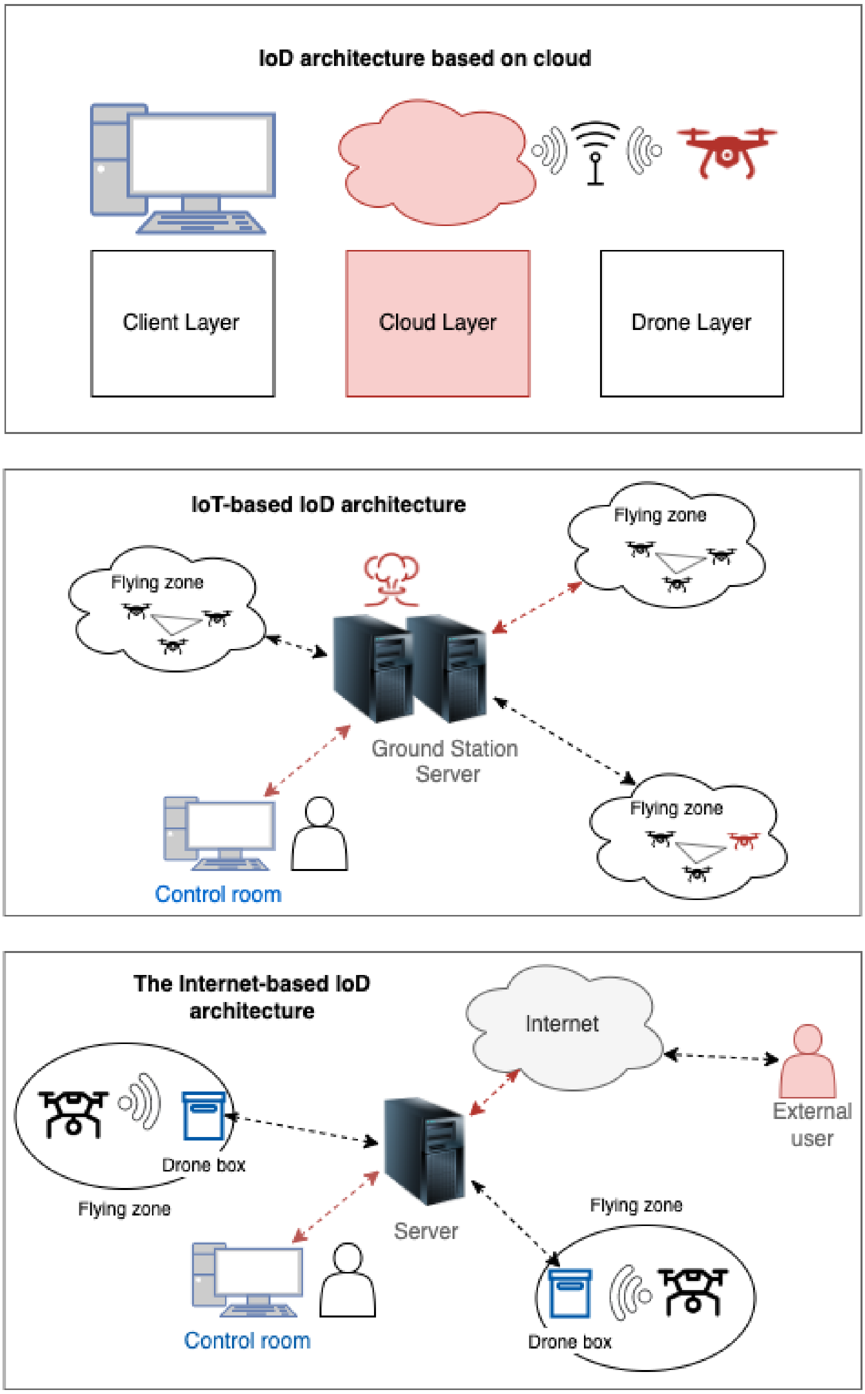


Figure 7.1: IoD architecture types with threats (adapted from [MRV22][OH22])

An illustration of some threats in an IoD network that were found during this thesis can be seen in Figure 7.2. It illustrates which elements are vulnerable to which threats, marked in red. The red elements include an adversary, a malicious drone, the data links, and a jammer. An adversary can use a jammer to disturb the IoD network, or it can occur unintentionally as one of the interviewees mentioned. The adversary can also perform replay attacks, preventing the UAV from receiving information. The malicious UAV can interfere with the IoD network. Threats to the IoD network include GPS spoofing, MITM, tampering, and eavesdropping among others.

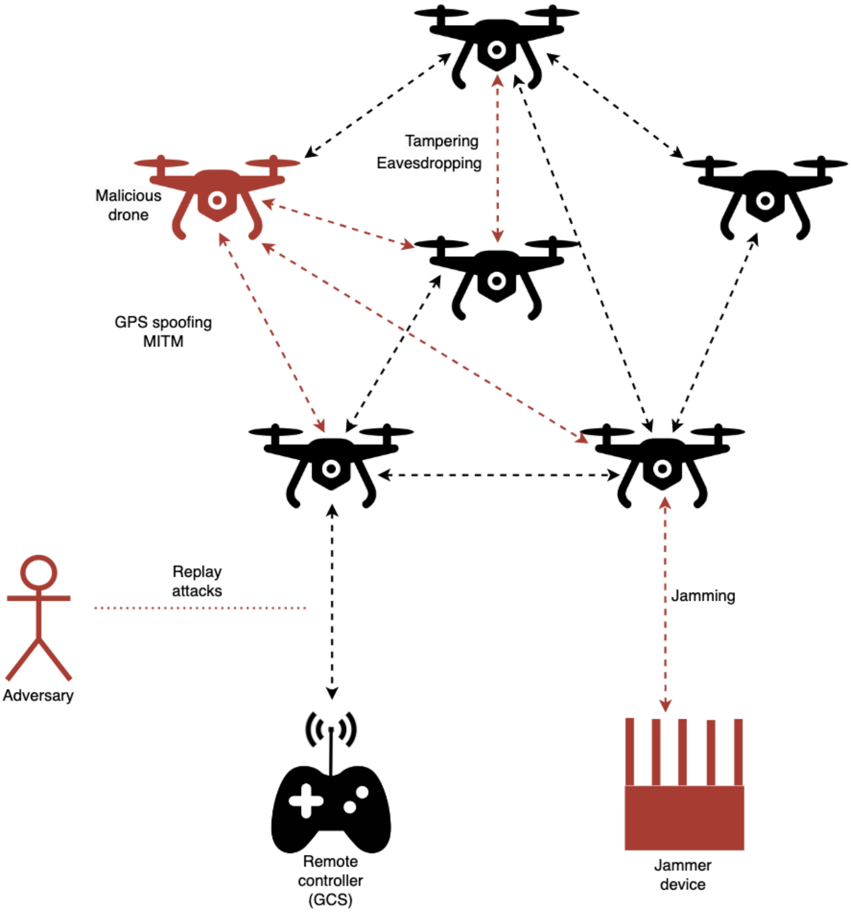


Figure 7.2: Some threats to IoD

During our pre-project [OH22], a table of threats to UAVs and IoD was conducted.

The table has been expanded in this thesis with several threats that were found, and amended with new security attributes, see Table 6.1. The table includes many of the threats mentioned in Section 3.3.2, and other threats that were found in the literature studies. It shows the target component(s) of the UAV and IoD, and which cybersecurity attribute(s) they affect. The threats identify the impact on Confidentiality (C), Integrity (I), Availability (A), Non-Repudiation (NR), Authenticity (Au), and Privacy (P).

In a UAV, the communication module, data link, payload, and sensors like the GPS will be prominent to attacks because they receive external information [MRV22]. For IoD, the target components include networks, services, and the platform. The platform refers to the infrastructure that enables the operation of the UAVs. An example of a platform is PX4 Autopilot, which was used in the experiments. The threats targeting the UAV components also apply to the IoD network since it consists of several UAVs.

Threat	**UAV component(s)**	**IoD component(s)**	**C**	**I**	**A**	**NR**	**Au**	**P**	**Reference**
GPS spoofing	GPS, Data Link	Networks, Platform, Services		✓	✓	✓	✓		[HAR22]
GPS jamming	GPS, Data Link	Services			✓	✓			[Kal22][HAR22]
DoS	Communication Module, Payload, Data Link	Networks, Platform, Services			✓	✓			[WA19][HAR22]
Hijacking	Communication Module, Payload	Networks, Platform, Services	✓	✓	✓		✓	✓	[WA19]
Replay attacks	Data Link	Networks		✓		✓	✓	✓	[TGV22]
Man in the Middle	Communication Module, Data Link	Networks, Platforms	✓	✓		✓	✓	✓	[YWY+22][CSG+18]
Eavesdropping	Data Link	Networks	✓					✓	[TGV22][Cos22]
Information Collision attacks	Data Link	Platform, Services			✓				[YWY+22]
Selective Forwarding	Communication Module, Data Link	Networks	✓		✓	✓	✓		[YWY+22]
Tampering attacks	Data Link	Services	✓	✓			✓	✓	[YWY+22]
ADS-B spoofing	ADS-B, Communication module	Networks, Platform	✓	✓	✓		✓		[YMB+19][HAR22]
Malicious drone in IoD network	N/A	Networks, Platform, Services	✓	✓	✓	✓			[YWY+22]
Physical tampering of the UAVs	Payload	Network, Services		✓	✓				[Ale21]
"Keylogging"/Computer virus	Payload	Platform	✓				✓	✓	[HS13]
Weakness in AI for swarm technology	Communication module	Network, Platform, Services	✓		✓				[Kal22]
Weakness in cloud	N/A	Network	✓	✓		✓		✓	[MRV22]
ARP spoofing	Communication Module	Services		✓		✓	✓		[SVG+22]

Table 7.1: Cybersecurity threats related to UAVs and the IoD

Chapter 8 Discussion

This chapter discusses the findings and how they answer the following research questions presented in the introduction:

RQ1 What are the security risks when it comes to the use of IoD within critical infrastructure?

RQ2 How difficult would it be to exploit the UAVs both technically and from a resource and a cost perspective?

RQ3 What mitigations can be applied to the IoD to overcome these risks?

We used a combination of the different methodologies to answer the questions. Interviews were a good tool to get insight and perspectives from people with knowledge within the UAVs field, and their thoughts around IoD and the use within critical infrastructure. Thus, they can in combination with the literature studies provide answers to **RQ1**. The experiments gave an idea of how easy or difficult it could be to perform attacks on UAVs and hence were meant to answer **RQ2**. Proposed mitigation techniques were also mentioned in the interviews, that together with the literature studies can be used to answer **RQ3**. Moreover, the validity of the results is discussed, and lastly, some thesis limitations are mentioned at the end of the chapter to enlighten what part(s) was challenging.

8.1 RQ1 - What are the security risks when it comes to the use of IoD within critical infrastructure?

Some of the primary concerns with using IoD in critical infrastructure are the potential for unauthorized access and control, in addition to disruption of the services. We can conclude from the interviews that many of the risks that are present in a single UAV are present in the IoD as well. The most prominent risks include GPS spoofing, jamming, hijacking, and DoS, which are present according to the literature review too. Interviewees mentioned that they had experienced repeated incidents of GPS jamming and DoS attacks, so we believe these threats are present in the real world to some degree, depending on the setting and use case. The literature review also mentioned other threats like MITM, eavesdropping, and ADS-B attacks, that the interviewees were not that familiar with.

The literature studies gave us an understanding that IoD is useful to gather a huge amount of data, including sensor readings, video footage, and location information. This data can be sensitive, particularly when used in critical infrastructure operations. Without proper security mitigations, the data is vulnerable to interception and there is a risk that this data gets into the wrong hands. Also, there is a rising concern about Chinese-produced UAVs, as there is a certain unclarity about what happens with the data and who has access to it. Chinese and perhaps Iranian and Russian-produced UAVs are not suitable in some critical infrastructure applications, because you do not want other governments to get information about your critical infrastructure sites. If such UAVs were used for highly critical infrastructure, the foreign governments could for instance have the opportunity to harm the systems if they wanted to, as they could use the information gathered to launch targeted attacks on installations. The violation of data privacy and confidentiality is a security risk associated with the IoD for this purpose.

In critical infrastructure environments, regulation of the airspace is essential for safe and uninterrupted operations. From the interviews, it was apparent that people are concerned about fitting into the regulatory framework when utilizing IoD. There has been an urgent need for some mutual frameworks from a common European point of view. The regulation for how UAVs can operate simultaneously and integrate with manned aviation, known as U-space, took effect from January 2023, as explained in Chapter 3. There are still some years until the full automation between manned and unmanned aviation will take place. We believe that this, in addition to new regulations on UAV operations, restricts the full potential of IoD. People and companies need time to adapt to the new regulations, and since the IoD is an emerging technology, regulations may need to be adapted over time.

Based on the interviews, our conclusion is that there are currently no specific threats related to IoD in critical infrastructure, as the technology is still in its early stages at the time of writing. However, potential threats in the future would mainly be unauthorized access of the UAVs caused by GPS spoofing and hijacking, disruption of services caused by jamming and DoS, and violation of data privacy. When it comes to using single UAVs for this purpose, this is already deployed and can have various consequences if compromised. For instance, in critical infrastructure sites, there could exist zones that are flammable with explosives and gasses and there is a risk of the UAVs flying into those areas. Cyberattacks could have fatal consequences in such scenarios.

8.2 RQ2 - How difficult would it be to exploit the UAVs both technically and from a resource and a cost perspective?

We identify the difficulty of exploiting the UAVs both technically and from a resource and cost perspective by analyzing our results from the experiments and the RCM, focusing on GPS spoofing and DoS attacks. It is challenging to exploit the UAVs technically, and some attacks require a significant cost and resources.

To exploit the UAVs technically, the attacker must have knowledge of the communication protocols and how a UAV receives messages. This is not straightforward and requires some research to figure out. If a person has significant knowledge about UAVs and software that can be used to program them, it would be easier to exploit them technically. Our code in the experiments was run with SITL, but it could also be modified to run on a real UAV. This is assumably more difficult than exploiting the UAVs in a simulation. Since the tools used were publicly available and free, we assume that an attacker in category 1 defined in Section 3.3.3, for example, a “script kiddie” or “hobbyist”, could spoof simulated UAVs, however, this could be impossible for him to accomplish on a real UAV.

The results from the experiments show that the course of the spoofed UAV got interrupted from its planned autonomous mission. If there were more UAVs in the air, the risk of collisions would be greater. GPS spoofing can enable an attacker to take control of the UAV by making it fly to him, or make it crash into an installation or flammable object to destroy infrastructure. This scenario was illustrated by spoofing the GPS signal of the UAV making it fly to SINTEF. The GPS spoofing attack was carried out after a thorough investigation of the software used and hence would be possible to replicate with the code attached in Appendix C and substantial knowledge of the software used.

During the experiments, we did not implement any algorithm that made the UAVs communicate because we wanted to focus on the cyberattack aspect of the UAVs. However, the implementation of such an algorithm would likely increase the difficulty of exploiting the UAVs if the algorithm was designed to withstand specific attacks or failures. Then, the IoD network could know that something had happened to one or more UAVs, as they would likely know where the other UAVs are situated.

If a stage in the RCM model requires a huge amount of work to be carried out or has a high associated cost, it could prevent an attacker from being able to execute the planned attack, like for instance, the DoS reconnaissance step which required a lot of resources. It can also provide an overview of the vulnerabilities present in the system to be attacked. By hardening wireless communication by using a non-default and strong password, the attack would be even more difficult and costly to carry out. That is an easy mitigation step with a big impact. The cost intervals facilitate the identification of the most probable threat agents to carry out such attacks as detailed hereafter.

GPS spoofing can be relatively cheap, as well as expensive. Using the cheaper resource alternatives with a cost of $1260, GPS spoofing a UAV should be achievable by threat actors belonging to category 2, the so-called "hacktivists" and "cyber criminals". We assume this equipment is enough to spoof commercial UAVs. For the more expensive resource alternatives, with a maximum price of $84 556, it is not unlikely that these can be used to compromise UAVs with greater security features implemented. This makes them achievable for attackers in category 3, namely the nation-state actors that have a lot of means, and almost unlimited resources. GPS spoofing of UAVs by nation-state actors have indeed been observed, and an example is the Iranian capture of American UAVs mentioned in Chapter 3.

The maximum cost to perform a DoS attack to a UAV is estimated to be around $9250, which would be a significant expense to an attacker belonging to category 1 or 2. However, a threat actor in category 1 would be able to execute the DoS attack by using the cheapest resource alternatives, which has a total cost of $130. If a threat actor in category 1 can successfully complete the DoS attack, the threat actors in the other two categories are also able to do so, however, the impact could be greater for the latter categories as they have the capability to execute a stealthier and larger-scale attack.

Analyzing the resource trees, jamming of the UAVs would be feasible by attackers in all categories, as the minimum cost of a jammer was $50. Some additional resources would be needed, but we assume that the cost would not be too great. However, we assume that a cheap jammer would not have the longest transmission range, so the impact is debatable.

To answer **RQ2**, it is quite difficult to exploit the UAVs technically, but it is feasible with the right knowledge and research. A lot of time went into understanding the software, and that would be the case for someone who does not have much experience with drone programming. As a result, we believe most hackers in category 1 would not be able to compromise real UAVs with a GPS spoofing attack. For the exploitation of the UAVs from a resource and cost perspective, we conclude that an attacker has to invest in some minimum resources that have an associated cost. The difficulty of this depends on the level of required resources. The more resources, the harder it is for an attacker to complete the attack. The attack could fail as early as in the reconnaissance stage if there are several resources required there.

8.3 RQ3 - What mitigations can be applied to the IoD to overcome these risks?

There are several mitigations that can be applied to the IoD, and the most apparent are encryption of the communication and the data, secure authentication, and strong credentials.

The goal is to build an IoD network more resilient to attacks. An advantage of IoD networks is the potential increased resiliency against some cyberattacks because of intercommunication between the UAVs. Attacks to a UAV in IoD would therefore not have as big impact as they would on a standalone UAV. For instance, GPS jamming or spoofing could be easier to detect and the group could build resiliency. If a UAV loses services, other UAVs can provide help.

During the interviews, it was mentioned that to overcome GPS spoofing, one can develop an algorithm that can decide if the signals are to be trusted based on the signal strength. If they are too high, it is unlikely that they come from space, hence the signals cannot be trusted. From the literature studies, intrusion detection could detect attacks to the UAV itself, and collision avoidance can mitigate collisions in the networks if the GPS were to be spoofed.

Furthermore, to overcome jamming, an interviewee mentioned that researchers have built the world's largest database on jamming events on satellite signals. This can potentially be used to overcome jamming signals in IoD. The interviews also revealed that jamming a UAV on 5G might pose a greater difficulty, as the UAV can be switched to manual mode, enabling it to safely return to its designated home location. In addition, the interviews indicated that carefully selecting the radio frequency and use a non-standard frequency can protect the UAV from jamming.

When using DJI UAVs, a countermeasure to avoid attacks can be to hide the broadcasted GPS position by modifying them to zero. In that way, the attacker has no straightforward knowledge about where the UAV is located. This can protect against attacks where the attacker needs to know the location of the UAV, like for instance GPS spoofing.

Changing the default credentials is also seen as a top priority, as a difficult password would be time-consuming to crack, and could be a mitigation against DoS attacks. If the UAV uses WiFi, a secure WiFi protocol should be used. IDSs can also be implemented to detect and stop DoS attacks.

In the event of hijacking, almost all best practices that are applicable to IoT could also be applied to IoD. Furthermore, encryption was mentioned in the interviews as a countermeasure to prevent the attacker from downloading the software and reading the data. Encryption can also provide confidentiality of the communication and make it unreadable to eavesdroppers. The interview findings also stated that removing access to the Internet when it is not needed can be a preventive measure against a UAV being compromised.

During the literature studies in Section 3.7, several mitigations that can be applied to the IoD network were found. Access control, lightweight authentication, cryptography-based authentication, privacy-preserving authentication, and blockchain-powered solution are some. By implementing robust security strategies, the potential risks can be minimized and the benefits of the IoD can be fully realized.

8.4 Validity of Results

8.4.1 Interviews

For this thesis, seven people were interviewed. Through their valuable insights and experiences, we obtained a comprehensive understanding of the challenges, opportunities, and best practices associated with UAV and IoD utilization, threats, and mitigations. It is important to note that the results from the interviews reflect their perspectives, and do not represent the UAV sector as a whole. Also, as the cybersecurity strategies applied for UAVs may be different in a research organization than in a drone company, this has resulted in a broader coverage of the topic, and some things might be misleading or incorrect in some circumstances.

8.4.2 Experiments

The experiments were performed on simulated UAVs, and not on real UAVs, as we did not have the equipment available. Therefore, our findings are not directly transferable to real-life attacks on UAVs.

8.4.3 Resource Cost Modeling

Resource cost modeling provides an idea of how cheap or expensive a cyberattack can be, and an estimate of the feasibility. However, as the CKC was primarily intended to estimate malware attacks, the RCM does not fit 100% to our attacks. For that reason, some steps lack a resource tree or associated resource alternatives.

A challenge with the RCM is that the costs and confidence values are subject to variation depending on who are carrying out the modeling and their personal opinions. Furthermore, the resource cost intervals for the resource alternatives were retrieved from online websites, and we did not take the delivery costs into account, nor considered any costs related to customs fees from foreign suppliers. This means that the associated costs would potentially be higher. Developing a script would have an unknown duration and depend on the attacker's skills. Hence, the costs estimated for this are somewhat uncertain. In addition, online prices are subject to variations, and therefore the estimations would be less precise.

Although the RCM carries certain restrictions, we believe that it remains a valuable tool for evaluating the cybersecurity aspects of a system. For operators of critical infrastructure and other users of UAVs and IoD, the model can provide a valuable understanding of the feasibility of potential attacks, considering the complexity of the attacks and associated costs.

8.5 Thesis Limitations

Our experiments were limited to the simulation of GPS spoofing attacks on UAVs. A limitation regarding the simulations was time, as this is mostly due to the steep learning curve of the software as we were unfamiliar with UAV simulation software. Due to this, we used a lot of time evaluating different software, and eventually on understanding how to operate the software, meaning PX4, Gazebo, ROS, and QGroundControl. Most files were written in C++, and this programming language is quite unfamiliar to us. However, ROS allows the creation of launch files and scripts in Python, which we have experience with. Despite this, ROS contained little examples and documentation on how to create files that we could use as inspiration for the attack, especially with Python. This restricted the simulation attacks to GPS spoofing only.

Chapter 9 Conclusion

9.1 Conclusion

UAVs provide numerous advantages but pose certain risks and challenges related to security. This study revealed that exploiting UAVs requires a significant level of expertise and knowledge of their operation in addition to having the skills to perform the attacks themselves. While it is indeed possible to exploit UAVs with adequate financial resources, the attempt can be perceived as challenging due to the complexity involved.

IoD is an emerging technology, and the adoption of IoD in critical infrastructure has the potential to revolutionize operations and efficiency. However, to fully take advantage of the benefits, it is essential to address the associated cybersecurity risks, and how different cyberattacks will affect the IoD. Unauthorized access and control of the UAVs caused by GPS spoofing and hijacking, as well as disruption of services caused by DoS attacks and jamming, and violation of data privacy, are the main potential cybersecurity threats when it comes to using IoD within critical infrastructure.

The consequences of cyberattacks can be severe to IoD applied in critical infrastructure, and services disrupted. This highlights the importance of a robust system together with countermeasures and mitigation strategies. By implementing a comprehensive security approach that includes robust authentication mechanisms, encryption protocols, jamming detection, and collision avoidance, the risks can be mitigated effectively, and ensure the safe and secure operations of IoD in critical infrastructure.

9.2 Future Work

Below are some proposals for future work that we considered while writing the thesis.

Perform GPS spoofing attacks on a network of communicating UAVs

Since **RQ2** focused on exploiting UAVs, not specifically IoD, it would be interesting to see how a UAV in an IoD network would be affected by GPS spoofing. This could provide an idea of the impact this would have.

Make one or more UAVs malicious in the IoD network

An interesting simulation scenario is to make one or more UAVs malicious in an IoD network and observe the consequences. Maybe it is possible to observe how many UAVs must be malicious to see a dangerous outcome.

Use the RCM on additional cyberattacks to UAVs/IoD

Utilizing the RCM on cyberattacks to UAVs that involve malware could be interesting, like for example a virus attack, as this model would apply better to such attacks. Then, the trees and associated costs would be more realistic.

References

[AGI+23] M. Abruzzese, S. Galasso, *et al.*, *Telematics-lab/IoD_sim*, original-date: 2021-11-11T13:22:01Z, Apr. 4, 2023. [Online]. Available: https://github.com/telematics-lab/IoD_Sim (last visited: Apr. 11, 2023).

[Ale21] Alex Apollonov, *Drone Darts are Silent and Deadly!*, Nov. 2021. [Online]. Available: https://www.youtube.com/watch?v=969XGZ_t7cE (last visited: Apr. 2, 2023).

[Ale23] R. P. Alex Fuller, «A roadmap to the next generation of uncrewed aviation», en, *NATS: BVLOS Operations Forum*, Mar. 2023. [Online]. Available: https://www.nats.aero/wp-content/uploads/2023/03/WhitePaper_South_of_the_clouds_March23.pdf (last visited: Apr. 29, 2023).

[AS20] A. F. AS, *Nytt dronesystem testes ved lufthavner i Norge – først ute i Nord-Europa | Avinor Flysikring AS*, no, 2020. [Online]. Available: https://kommunikasjon.ntb.no/pressemelding/nytt-dronesystem-testes-ved-lufthavner-i-norge-forst-ute-i-nord-europa?publisherId=17623239&releaseId=17890736 (last visited: Apr. 4, 2023).

[aut23a] P. autopilot. «Multi-vehicle simulation with ROS 2». (2023), [Online]. Available: https://docs.px4.io/main/en/ros/ros2_multi_vehicle.html (last visited: May 1, 2023).

[aut23b] P. autopilot. «ROS 2 user guide». (2023), [Online]. Available: https://docs.px4.io/main/en/ros/ros2_comm.html (last visited: May 1, 2023).

[BCD20] B. Bera, D. Chattaraj, and A. K. Das, «Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment», en, *Computer Communications*, vol. 153, pp. 229–249, Mar. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366419318377 (last visited: Feb. 10, 2023).

[CIS] CIS, *Cybersecurity spotlight - cyber threat actors*, CIS: Center for Internet Security. [Online]. Available: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/ (last visited: Feb. 15, 2023).

[CIS19] CISA. «What is cybersecurity? | CISA». (Nov. 2019), [Online]. Available: hhttps://www.cisa.gov/news-events/news/what-cybersecurity (last visited: Feb. 6, 2023).

[Coa23] U. Coach, *Top 100 Drone Companies to Watch in 2023*, en-US, 2023. [Online]. Available: https://uavcoach.com/drone-companies/ (last visited: Mar. 26, 2023).

[Com] T. D. Company, *Volunteer Ukrainian Drone Unit: "We Are All Soldiers Now"*. [Online]. Available: https://thedroningcompany.com/blog/thedroningcompany.com/blog/volunteer-ukrainian-drone-unit-we-are-all-soldiers-now (last visited: Jun. 5, 2023).

[Cos22] A. Costin, «Insecure firmware and wireless technologies as "achilles' heel" in cybersecurity of cyber-physical systems», in *Cyber Security: Critical Infrastructure Protection*, ser. Computational Methods in Applied Sciences, M. Lehto and P. Neittaanmäki, Eds., Cham: Springer International Publishing, 2022, pp. 419–443. [Online]. Available: https://doi.org/10.1007/978-3-030-91293-2_18 (last visited: Feb. 16, 2023).

[CSG+18] G. Choudhary, V. Sharma, *et al.*, «Internet of Drones (IoD): Threats, Vulnerability, and Security Perspectives», in *MobiSec 2018: The 3rd International Symposium on Mobile Internet Security*, Aug. 2018.

[CW19] Y.-J. Chen and L.-C. Wang, «Privacy Protection for Internet of Drones: A Network Coding Approach», *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1719–1730, Apr. 2019, Conference Name: IEEE Internet of Things Journal.

[CYK+21] S. A. Chaudhry, K. Yahya, *et al.*, «GCACS-IoD: A certificate based generic access control scheme for Internet of drones», en, *Computer Networks*, vol. 191, p. 107 999, May 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621001195 (last visited: Feb. 1, 2023).

[DJI15] DJI, *Phantom3 user manual v1.4*, 2015. [Online]. Available: https://dl.djicdn.com/downloads/phantom_3_standard/en/Phantom_3_Standard_User_Manual_v1.4_en_0112.pdf (last visited: May 24, 2023).

[DNV22] DNV, «The cyber priority», p. 17, May 2022, Conference Name: IEEE Internet of Things Journal.

[DV19] M. DeJonckheere and L. M. Vaughn, «Semistructured interviewing in primary care research: A balance of relationship and rigour», *Family Medicine and Community Health*, vol. 7, no. 2, e000057, Mar. 1, 2019, Publisher: BMJ Specialist Journals Section: Methodology. [Online]. Available: https://fmch.bmj.com/content/7/2/e000057 (last visited: May 5, 2023).

[Eus19] A. G. Eustis, «The mirai botnet and the importance of IoT device security», in *16th International Conference on Information Technology-New Generations (ITNG 2019)*, S. Latifi, Ed., ser. Advances in Intelligent Systems and Computing, Cham: Springer International Publishing, 2019, pp. 85–89.

[Gar21] M. Gargalakos, «The role of unmanned aerial vehicles in military communications: Application scenarios, current trends, and beyond», *The Journal of Defense Modeling and Simulation*, p. 15 485 129 211 031 668, Jul. 2021, Publisher: SAGE Publications. [Online]. Available: https://doi.org/10.1177/15485129211031668 (last visited: Mar. 30, 2023).

[GBW16] M. Gharibi, R. Boutaba, and S. L. Waslander, «Internet of Drones», *IEEE Access*, vol. 4, pp. 1148–1162, 2016, Conference Name: IEEE Access.

[GIBG22] G. Grieco, G. Iacovelli, *et al.*, *Internet of Drones Simulator: Design, Implementation, and Performance Evaluation.* Mar. 25, 2022.

[Gro21] S. M. Group, *Does Your UAV Program Need a Transponder?*, en, May 1, 2021. [Online]. Available: https://www.mobilityengineeringtech.com/component/content/article/adt/pub/features/articles/39050 (last visited: Nov. 7, 2022).

[Hag20] K. Haga, «Breaking the Cyber Kill Chain by Modelling Resource Costs», M.S. thesis, NTNU Department of Computer Science, Jun. 2020.

[HAR22] M. Haider, I. Ahmed, and D. B. Rawat, «Cyber Threats and Cybersecurity Reassessed in UAV-assisted Cyber Physical Systems», in *2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, ISSN: 2165-8536, Jul. 2022, pp. 222–227.

[Haw21] J. Hawdon, «Cybercrime: Victimization, perpetration, and techniques», *American Journal of Criminal Justice*, vol. 46, no. 6, pp. 837–842, 2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8579169/ (last visited: Feb. 13, 2023).

[HCA+21a] V. Hassija, V. Chamola, *et al.*, «Fast, reliable, and secure drone communication: A comprehensive survey», *IEEE Communications Surveys & Tutorials*, vol. PP, Jul. 13, 2021.

[HCA+21b] S. Hussain, S. A. Chaudhry, *et al.*, «Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones», *IEEE Systems Journal*, vol. 15, pp. 4431–4438, Sep. 2021, Conference Name: IEEE Systems Journal.

[HCA11] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, «Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains», in *Leading Issues in Information Warfare and Security Research.* Academic Publishing International Limited, 2011, vol. 1.

[HE16] J. Hoekstra and J. Ellerbroek, «BlueSky ATC simulator project: An open data and open source approach», Jun. 21, 2016.

[HMS20] K. Haga, P. H. Meland, and G. Sindre, «Breaking the cyber kill chain by modelling resource costs», in *Graphical Models for Security*, H. Eades III and O. Gadyatskaya, Eds., ser. Lecture Notes in Computer Science, Cham: Springer International Publishing, Nov. 2020, pp. 111–126.

[HOM21] Y. Haddad, E. Orye, and O. Maennel, «Ghost injection attack on automatic dependent surveillance–broadcast equipped drones impact on human behaviour», in *2021 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, ISSN: 2379-1675, May 2021, pp. 161–166.

[HRW22] HRW. «Ukraine: Russian attacks on energy grid threaten civilians», Human Rights Watch. (Dec. 6, 2022), [Online]. Available: https://www.hrw.org/news/2022/12/06/ukraine-russian-attacks-energy-grid-threaten-civilians (last visited: Feb. 27, 2023).

[HS13] K. Hartmann and C. Steup, «The vulnerability of UAVs to cyber attacks - An approach to the risk assessment», in *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, ISSN: 2325-5374, Jun. 2013, pp. 1–23.

[INS22] M. INSIDER. «What is software-in-the-loop testing?», Aptiv. (2022), [Online]. Available: https://www.aptiv.com/en/insights/article/what-is-software-in-the-loop-testing (last visited: May 9, 2023).

[ITU] ITU, *Cybersecurity*, ITU. [Online]. Available: https://www.itu.int:443/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (last visited: Feb. 6, 2023).

[JZR22] S. M. Jameii, R. S. Zamirnaddafi, and R. Rezabakhsh, «Internet of flying things security: A systematic review», *Concurrency and Computation: Practice and Experience*, vol. 34, no. 24, e7213, 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.7213 (last visited: Jun. 10, 2023).

[Kal22] Z. Kallenborn, *From Electronic Warfare to Cyber and Beyond: How Drones Intersect with the Information Environment on the Battlefield*, en-US, Apr. 2022. [Online]. Available: https://mwi.usma.edu/from-electronic-warfare-to-cyber-and-beyond-how-drones-intersect-with-the-information-environment-on-the-battlefield/ (last visited: Feb. 7, 2023).

[Kar22] A. P. Karanja, *How to Detect a Drone in the Sky*, en-US, Section: Articles, Mar. 2022. [Online]. Available: https://www.droneblog.com/detect-a-drone/ (last visited: May 15, 2023).

[KKN+21] A. Kumar, R. Krishnamurthi, *et al.*, «A novel Software-Defined Drone Network (SDDN)-based collision avoidance strategies for on-road traffic monitoring and management», en, *Vehicular Communications*, vol. 28, p. 100 313, Apr. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221420962030084X (last visited: Feb. 8, 2023).

[KL22] S. Kimathi and B. Lantos, «Unmanned aerial vehicles swarm flocking architectures: An overview», in *2022 IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC)*, Jul. 2022, pp. 000 383–000 388.

[Knu] A. Knutsen, *Unammed traffic management: Ninox drone - how are we handling drones for the future?*, no. [Online]. Available: https://luftfartstilsynet.no/globalassets/dokumenter/dronedokumenter/arrangement/2---avinor-ninox---axel.pdf (last visited: Apr. 4, 2023).

[KS21] N. Kolokotronis and S. Shiaeles, *Cyber-Security Threats, Actors, and Dynamic Mitigation.* CRC Press, Apr. 4, 2021, 392 pp., Google-Books-ID: FX-UhEAAAQBAJ.

[Leh22] M. Lehto, «Cyber-attacks against critical infrastructure», in *Cyber Security: Critical Infrastructure Protection*, ser. Computational Methods in Applied Sciences, M. Lehto and P. Neittaanmäki, Eds., Springer International Publishing, 2022, pp. 3–42. [Online]. Available: https://doi.org/10.1007/978-3-030-91293-2_1 (last visited: Feb. 16, 2023).

[Lufa] Luftfartstilsynet, *Guide for flying drones in Norway - Overview | Rise 360*. [Online]. Available: https://rise.articulate.com/share/H0ZTFmqESotDUeD3ndHHPz1mjeainQKK#/ (last visited: Mar. 26, 2023).

[Lufb] Luftfartstilsynet, *Registrer | Flydrone*. [Online]. Available: https://flydrone.no/register (last visited: Mar. 26, 2023).

[Luf22] Luftfartstilsynet, *Dronepilot A1/A3: Dronepilot A1/A3*, https://kurs.caa.no/, 2022. [Online]. Available: https://kurs.caa.no/ (last visited: Sep. 28, 2022).

[Mar15] L. Martin, *Gaining The Advantage - Applying the Cyber Kill Chain® Methodology to Network Defence*, 2015. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf (last visited: Jan. 31, 2023).

[Mar22a] L. Martin. «About us», Lockheed Martin. (Sep. 27, 2022), [Online]. Available: https://www.lockheedmartin.com/en-us/who-we-are.html (last visited: Jan. 31, 2023).

[Mar22b] L. Martin. «Cyber Kill Chain®». (Jun. 2022), [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (last visited: Jan. 30, 2023).

[Mar23] MarketsandMarkets, *Drone Inspection and Monitoring Market Size, Share, Growth Drivers, Analysis - 2030*, Feb. 2023. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/drone-inspection-monitoring-market-99915267.html (last visited: Mar. 27, 2023).

[MM20] P. Maynard and K. McLaughlin, «Big fish, little fish, critical infrastructure: An analysis of phineas fisher and the 'hacktivist' threat to critical infrastructure», in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Jun. 2020, pp. 1–7.

[MRV22] S. Maurya, M. M. S. Rauthan, and R. Verma, «Security aspects of the internet of drones (IoD)», in *2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, Apr. 2022, pp. 1–6.

[MVC+16] R. Miani, G. Vasconcelos, *et al.*, *The Impact of DoS Attacks on the AR.Drone 2.0.* Dec. 2016.

[Nea18] A. Neal, *LiDAR vs. RADAR*, en, Apr. 2018. [Online]. Available: https://www.fierceelectronics.com/components/lidar-vs-radar (last visited: Feb. 8, 2023).

[Nor22] H. Nord, «Drone use within critical infrastructure - a security perspective», M.S. thesis, Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering, 2022. [Online]. Available: http://ltu.diva-portal.org/smash/get/diva2:1682334/FULLTEXT01.pdf (last visited: Oct. 24, 2022).

[OH22] L. E. Omli-Moe and J. D. Hjelle, «Cybersecurity Threats to Unmanned Aerial Vehicles», Department of Information Security, Communication Technology, NTNU – Norwegian University of Science, and Technology, Project report in TTM4502, Dec. 2022.

[Osb23] K. Osborn, *New Air Force 6th-Gen Stealth Fighter Will Control 5 Drones*, en, Jan. 2023. [Online]. Available: https://warriormaven.com/air/-air-force-6th-gen-stealth-fighter-drones (last visited: Apr. 6, 2023).

[Par] Parrot, *Parrot AR.drone default password & login, and reset instructions.* [Online]. Available: //www.router-reset.com/info/Parrot/ARDrone (last visited: May 24, 2023).

[Pol23] Politiforum, «Hvordan skal vi stoppe dronene?», p. 98, 2023.

[Pro] D. Project, *Introduction - MAVLink developer guide.* [Online]. Available: https://mavlink.io/en/ (last visited: May 10, 2023).

[PW17] D. Park and M. Walstrom. «Cyberattack on critical infrastructure: Russia and the ukrainian power grid attacks», University of Washington. (Oct. 11, 2017), [Online]. Available: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/ (last visited: Feb. 27, 2023).

[PX423a] PX4. «ROS 2 offboard control example». (Mar. 2023), [Online]. Available: https://docs.px4.io/main/en/ros/ros2_offboard_control.html (last visited: May 1, 2023).

[PX423b] PX4. «ROS with gazebo classic simulation». (Mar. 2023), [Online]. Available: https://docs.px4.io/main/en/simulation/ros_interface.html (last visited: May 30, 2023).

[RBJ20] G. Rongxiao, W. Buhong, and W. Jiang, «Vulnerabilities and Attacks of UAV Cyber Physical Systems», in *CNIOT2020: International Conference on Computing, Networks and Internet of Things*, Apr. 2020, pp. 8–12. [Online]. Available: https://dl.acm.org/doi/epdf/10.1145/3398329.3398331 (last visited: Feb. 6, 2023).

[REAE21] R. A. Ramadan, A.-H. Emara, *et al.*, «Internet of Drones Intrusion Detection Using Deep Learning», en, *Electronics*, vol. 10, no. 21, p. 2633, Jan. 2021, Number: 21 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/2079-9292/10/21/2633 (last visited: Feb. 13, 2023).

[Reg17] Regjeringen, *Forordning om U-space*, no, EOSnotat, Publisher: regjeringen.no, Aug. 2017. [Online]. Available: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2017/aug/u-space/id2570869/ (last visited: Apr. 4, 2023).

[Rin19] D. Ringquist, «Script kiddies», in *Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, and Technology*, N. M. Sambaluk, Ed., ABC-CLIO, 2019.

[Rob] 3. Robotics, *About DroneKit.* [Online]. Available: https://dronekit-python.readthedocs.io/en/latest/about/overview.html (last visited: Apr. 11, 2023).

[ROS18] ROS. «Nodes - ROS wiki». (2018), [Online]. Available: http://wiki.ros.org/Nodes (last visited: May 1, 2023).

[Rus16] M.-A. Russon. «Police drones can be hacked and stolen from 2km away by hijacking on-board chips», International Business Times UK. Section: CyberSecurity. (Apr. 4, 2016), [Online]. Available: https://www.ibtimes.co.uk/police-drones-can-be-hacked-stolen-2km-away-by-hijacking-board-chips-1553122 (last visited: May 21, 2023).

[Sch99] B. Schneier, *Attack Trees*, Dec. 1999. [Online]. Available: https://tnlandforms.us/cs594-cns96/attacktrees.pdf (last visited: Feb. 2, 2023).

[SCS+22] N. Schiller, M. Chlosta, *et al.*, «Drone security and the mysterious case of DJI's DroneID», in *Network and Distributed System Security Symposium (NDSS)*, 2022. [Online]. Available: https://mu00d8.me/paper/schiller23dronesecurity.pdf.

[SDKR19] J. Srinivas, A. K. Das, *et al.*, «TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment», *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019, Conference Name: IEEE Transactions on Vehicular Technology.

[SIN22] SINTEF, «IoT security checklist», 2022. [Online]. Available: https://www.sintef.no/contentassets/8fa5c7e3a81749b8952979000ee34c31/iot-security-checklist-v1.1.0.pdf.

[Sok16] S. Sokol, *Ghost In The Machine*, en-US, Jun. 2016. [Online]. Available: https://www.falkenavionics.com/ghost-in-the-machine/ (last visited: Apr. 6, 2023).

[Sta17] W. Stallings, *Cryptography and network security: principles and practice*, Seventh edition. Boston: Pearson, 2017, 748 pp.

[Sto22] K. Stoddart, «Introduction», in *Cyberwarfare: Threats to Critical Infrastructure*, ser. Palgrave Studies in Cybercrime and Cybersecurity, K. Stoddart, Ed., Cham: Springer International Publishing, 2022, pp. 1–51. [Online]. Available: https://doi.org/10.1007/978-3-030-97299-8_1 (last visited: Feb. 20, 2023).

[Sto23a] K. Stormark, *395 dronemeldinger på et halvt år*, Section: nyheter, Feb. 2023. [Online]. Available: https://www.politiforum.no/395-dronemeldinger-pa-et-halvt-ar/236079 (last visited: Mar. 7, 2023).

[Sto23b] K. Stormark, *Dronebølgen*, nb-no, Section: nyheter, Mar. 2023. [Online]. Available: https://www.politiforum.no/dronebolgen/236136 (last visited: Mar. 6, 2023).

[Sto23c] K. Stormark, *Forvarslene*, nb-no, Section: nyheter, Feb. 2023. [Online]. Available: https://www.politiforum.no/forvarslene/236092 (last visited: Mar. 6, 2023).

[Sto23d] K. Stormark, *Hvem skal stanse dronene?*, Section: nyheter, Mar. 2023. [Online]. Available: https://www.politiforum.no/hvem-skal-stanse-dronene/236206 (last visited: Mar. 6, 2023).

[Sto23e] K. Stormark, *Slik etterforsket de dronehendelsene*, Section: nyheter, Mar. 2023. [Online]. Available: https://www.politiforum.no/slik-etterforsket-de-dronehendelsene/236181 (last visited: Mar. 7, 2023).

[SVG+22] P. Solnør, Ø. Volden, *et al.*, «Hijacking of unmanned surface vehicles: A demonstration of attacks and countermeasures in the field», *Journal of Field Robotics*, vol. 39, no. 5, pp. 631–649, 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/rob.22068 (last visited: Jan. 31, 2023).

[Ted21] P. Tedeschi, «Security and privacy issues in internet of skies: Advanced solutions for drones and UAVs for critical infrastructures protection», ISBN: 9798790665905 Publication Title: PQDT - Global, Ph.D. dissertation, Hamad Bin Khalifa University (Qatar), Qatar, 2021, 190 pp. [Online]. Available: https://www.proquest.com/docview/2637141133/abstract/3D473D20A7C44A7EPQ/1 (last visited: Feb. 21, 2023).

[TGV22] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, «A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks», *Ad Hoc Networks*, vol. 133, p. 102 894, Aug. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870522000853 (last visited: Feb. 15, 2023).

[TS223] TS2, *How does a drone's fail-safe system work? – TS2 SPACE*, en-US, Feb. 21, 2023. [Online]. Available: https://ts2.space/en/how-does-a-drones-fail-safe-system-work/ (last visited: Jun. 5, 2023).

[TYS19] Y. Tian, J. Yuan, and H. Song, «Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones», en, *Journal of Information Security and Applications*, vol. 48, p. 102 354, Oct. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212618307038 (last visited: Feb. 10, 2023).

[Vac17] J. Vacca, *Computer and Information Security Handbook*, en. Morgan Kaufmann, May 2017, Google-Books-ID: 05HUDQAAQBAJ.

[VNBC16] B. Vergouw, H. Nagel, *et al.*, «Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments», in vol. 27, Oct. 2016, pp. 21–45.

[WA19] O. Westerlund and R. Asif, «Drone hacking with raspberry-pi 3 and WiFi pineapple: Security and privacy threats for the internet-of-things», in *2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)*, Feb. 2019, pp. 1–10.

[Way22] R. Wayman. «Compound annual growth rate: What you should know», Investopedia. (May 16, 2022), [Online]. Available: https://www.investopedia.com/investing/compound-annual-growth-rate-what-you-should-know/ (last visited: Jun. 1, 2023).

[WDL18] M. Wazid, A. K. Das, and J.-H. Lee, «Authentication protocols for the internet of drones: Taxonomy, analysis and future directions», en, *Journal of Ambient Intelligence and Humanized Computing*, Aug. 2018. [Online]. Available: https://doi.org/10.1007/s12652-018-1006-x (last visited: Apr. 29, 2023).

[WH20] A. Walde and E. G. Hanus, «The feasibility of AIS- and GNSS-based attacks within the maritime industry», eng, Accepted: 2021-09-23T19:06:59Z, M.S. thesis, NTNU, 2020. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2781145 (last visited: May 20, 2023).

[WIR15] WIRED. «Hackers remotely kill a jeep on a highway | WIRED». (Jul. 21, 2015), [Online]. Available: https://www.youtube.com/watch?v=MK0SrxBC1xs (last visited: Apr. 5, 2023).

[YIA+21] M. Yahuza, M. Y. I. Idris, *et al.*, «Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges», *IEEE Access*, vol. 9, pp. 57 243–57 270, 2021, Conference Name: IEEE Access.

[YMB+19] X. Ying, J. Mazer, *et al.*, *Detecting ADS-B Spoofing Attacks using Deep Neural Networks*, arXiv:1904.09969 [cs], Apr. 2019. [Online]. Available: http://arxiv.org/abs/1904.09969 (last visited: Feb. 8, 2022).

[YWY+22] W. Yang, S. Wang, *et al.*, «A Review on Security Issues and Solutions of the Internet of Drones», *IEEE Open Journal of the Computer Society*, vol. 3, pp. 96–110, 2022, Conference Name: IEEE Open Journal of the Computer Society.

[Zip] Zipline, *Zipline: Oversikt | LinkedIn.* [Online]. Available: https://www.linkedin.com/company/flyzipline/ (last visited: Apr. 4, 2023).

Appendix A
Interview guide

During our interviews, we used the common term “drones” instead of UAVs.

1. General about drones

- In what way can drones be used today? In what are you using drones today?
- What do you think are the benefits of using drones?
- What are the potential limitations of drones?
- What is the future outlook for drones?

2. Cyber threats related to drone usage

- What are the common types of cyber threats facing drones?
- What are the consequences of these cyber threats?
- What is the likelihood of these risks?
- How will these consequences change with IoD?

3. IoD

- In what scenarios could IoD be useful?
- What do you think are the benefits of switching to IoD?
- What can go wrong when using an IoD network?

4. Critical infrastructure

- How vulnerable do you think critical infrastructure, like for instance power lines or oil platforms, are to attacks/sabotage?
- Do you think the use of drones and/or IoD will reduce these risks? How/why?
- Why should companies operating critical infrastructure use IoD?
- Can you imagine some specific risks regarding the use of IoD within critical infrastructure?

5. Mitigations

- What mitigations do you foresee to the cyber risks related to drones?
- How do you think these mitigations will change with IoD?
- How can organizations effectively respond to a drone cyber attack?
- In your opinion, what steps need to be taken to ensure the security of drones in the future?

Appendix B
Mission Plan in Trondheim

```
{
    "fileType": "Plan",
    "geoFence": {
        "circles": [
        ],
        "polygons": [
        ],
        "version": 2
    },
    "groundStation": "QGroundControl",
    "mission": {
        "cruiseSpeed": 15,
        "firmwareType": 12,
        "globalPlanAltitudeMode": 1,
        "hoverSpeed": 5,
        "items": [
            {
                "AMSLAltAboveTerrain": null,
                "Altitude": 50,
                "AltitudeMode": 1,
                "autoContinue": true,
                "command": 22,
                "doJumpId": 1,
                "frame": 3,
                "params": [
                    0,
                    0,
                    0,
                    null,
                    63.4195043,
                10.4019248,
                50
            ],
            "type": "SimpleItem"
        },
        {
            "AMSLAltAboveTerrain": 50,
            "Altitude": 50,
            "AltitudeMode": 1,
            "autoContinue": true,
            "command": 16,
            "doJumpId": 2,
            "frame": 3,
            "params": [
                0,
                0,
                0,
                null,
                63.41678414,
                10.40527188,
                50
            ],
            "type": "SimpleItem"
        },
        {
            "AMSLAltAboveTerrain": 50,
            "Altitude": 50,
            "AltitudeMode": 1,
            "autoContinue": true,
            "command": 16,
            "doJumpId": 3,
            "frame": 3,
            "params": [
                0,
                0,
                0,
                null,
                63.42682384,
                10.41445154,
                50
            ],
        "type": "SimpleItem"
    },
    {
        "AMSLAltAboveTerrain": 50,
        "Altitude": 50,
        "AltitudeMode": 1,
        "autoContinue": true,
        "command": 16,
        "doJumpId": 4,
        "frame": 3,
        "params": [
            0,
            0,
            0,
            null,
            63.43407255,
            10.41354491,
            50
        ],
        "type": "SimpleItem"
    },
    {
        "AMSLAltAboveTerrain": 50,
        "Altitude": 50,
        "AltitudeMode": 1,
        "autoContinue": true,
        "command": 16,
        "doJumpId": 5,
        "frame": 3,
        "params": [
            0,
            0,
            0,
            null,
            63.4297641,
            10.39393898,
            50
        ],
        "type": "SimpleItem"
    },
    {
```

```
                "autoContinue": true,
                "command": 20,
                "doJumpId": 6,
                "frame": 2,
                "params": [
                    0,
                    0,
                    0,
                    0,
                    0,
                    0,
                    0
                ],
                "type": "SimpleItem"
            }
        ],
        "plannedHomePosition": [
            63.4195043,
            10.4019248,
            0
        ],
        "vehicleType": 2,
        "version": 2
    },
    "rallyPoints": {
        "points": [
        ],
        "version": 2
    },
    "version": 1
}
```

Appendix C
ROS 1 files

C.1 start_offb.launch

```
<?xml version="1.0"?>
<launch>
        <!-- Include the MAVROS node with SITL and Gazebo -->
        <include file="$(find px4)/launch/mavros_posix_sitl.launch">
            <arg name="world" default="$(find mavlink_sitl_gazebo)/
                worlds/trondheim.world"/>
        </include>

        <!-- Our node to control the drone -->
        <node pkg="offboard_py" type="offb_node.py" name="offb_node_py
            " required="true" output="screen" />
</launch>
```

C.2 spoofing.launch

```
<?xml version="1.0"?>
<launch>
        <!-- Our node to control the drone -->
        <node pkg="offboard_py" type="spoofing.py" name="
            spoofing_node_py" required="true" output="screen" />
</launch>
```

C.3 offb_node.py

```
#! /usr/bin/python3

import rospy
from geometry_msgs.msg import PoseStamped
from mavros_msgs.msg import State
from mavros_msgs.srv import CommandBool, CommandBoolRequest, SetMode,
     SetModeRequest

current_state = State()

def state_cb(msg):
    global current_state
    current_state = msg


if __name__ == "__main__":
    rospy.init_node("offb_node_py")

    state_sub = rospy.Subscriber("mavros/state", State, callback =
        state_cb)

    local_pos_pub = rospy.Publisher("mavros/setpoint_position/local",
         PoseStamped, queue_size=10)
    rospy.wait_for_service("/mavros/cmd/arming")
    arming_client = rospy.ServiceProxy("mavros/cmd/arming",
        CommandBool)

    rospy.wait_for_service("/mavros/set_mode")
    set_mode_client = rospy.ServiceProxy("mavros/set_mode", SetMode)


    # Setpoint publishing MUST be faster than 2Hz
    rate = rospy.Rate(20)

    # Wait for Flight Controller connection
    while(not rospy.is_shutdown() and not current_state.connected):
        rate.sleep()

    pose = PoseStamped()

    pose.pose.position.x = 100
    pose.pose.position.y = 300
    pose.pose.position.z = 30
    # Send a few setpoints before starting
    for i in range(100):
        if(rospy.is_shutdown()):
            break

        local_pos_pub.publish(pose)
        rate.sleep()

    offb_set_mode = SetModeRequest()
    offb_set_mode.custom_mode = 'OFFBOARD'

    arm_cmd = CommandBoolRequest()
    arm_cmd.value = True

    last_req = rospy.Time.now()

    while(not rospy.is_shutdown()):
        if(current_state.mode != "OFFBOARD" and (rospy.Time.now() -
            last_req) > rospy.Duration(5.0)):
            if(set_mode_client.call(offb_set_mode).mode_sent == True):
                rospy.loginfo("OFFBOARD enabled")

            last_req = rospy.Time.now()
        else:
            if(not current_state.armed and (rospy.Time.now() -
                last_req) > rospy.Duration(5.0)):
                if(arming_client.call(arm_cmd).success == True):
                    rospy.loginfo("Vehicle armed")

                last_req = rospy.Time.now()

        local_pos_pub.publish(pose)
        rate.sleep()
```

C.4 spoofing.py

```
#! /usr/bin/python3

import rospy
from geographic_msgs.msg import GeoPoseStamped
from mavros_msgs.msg import State
from mavros_msgs.srv import CommandBool, CommandBoolRequest, SetMode,
     SetModeRequest

current_state = State()

def state_cb(msg):
    global current_state
    current_state = msg


if __name__ == "__main__":
    rospy.init_node("offb_node_py")

    state_sub = rospy.Subscriber("mavros/state", State, callback =
        state_cb)
    global_pos_pub = rospy.Publisher("/mavros/setpoint_position/
        global", GeoPoseStamped, queue_size=10 )
    rospy.wait_for_service("/mavros/cmd/arming")
    arming_client = rospy.ServiceProxy("mavros/cmd/arming",
        CommandBool)

    rospy.wait_for_service("/mavros/set_mode")
    set_mode_client = rospy.ServiceProxy("mavros/set_mode", SetMode)


    # Setpoint publishing MUST be faster than 2Hz
    rate = rospy.Rate(20)

    # Wait for Flight Controller connection
    while(not rospy.is_shutdown() and not current_state.connected):
        rate.sleep()

    geopose = GeoPoseStamped()

    geopose.pose.position.latitude = 63.413808006354735
    geopose.pose.position.longitude = 10.4111722559795
    geopose.pose.position.altitude = 30.0

    # Send a few setpoints before starting
    for i in range(100):
        if(rospy.is_shutdown()):
```

```
        break

    global_pos_pub.publish(geopose)
    rate.sleep()

offb_set_mode = SetModeRequest()
offb_set_mode.custom_mode = 'OFFBOARD'

arm_cmd = CommandBoolRequest()
arm_cmd.value = True

last_req = rospy.Time.now()

while(not rospy.is_shutdown()):
    if(current_state.mode != "OFFBOARD" and (rospy.Time.now() -
        last_req) > rospy.Duration(5.0)):
        if(set_mode_client.call(offb_set_mode).mode_sent == True):
            rospy.loginfo("OFFBOARD enabled")

        last_req = rospy.Time.now()
    else:
        if(not current_state.armed and (rospy.Time.now() -
            last_req) > rospy.Duration(5.0)):
            if(arming_client.call(arm_cmd).success == True):
                rospy.loginfo("Vehicle armed")

            last_req = rospy.Time.now()

    global_pos_pub.publish(geopose)
    rate.sleep()
```

NTNU

Norwegian University of
Science and Technology