Master's thesis

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

Aleksander Walde & Einar Gaustad Hanus

The feasibility of AIS- and GNSS-based attacks within the maritime industry

Master's thesis in Communication Technology and Digital Security
Supervisor: Karin Bernsmed
June 2020

NTNU
Norwegian University of Science and Technology

Title:	The feasibility of AIS- and GNSS-based attacks within the maritime industry
Student:	Aleksander Walde & Einar Gaustad Hanus

Problem description:

Global Navigation Satellite System (GNSS) and Automatic Identification System (AIS) are two of the main systems that are used by ships to avoid collision and achieve precise navigation when traveling. The systems are widely used in the shipping industry with over half a million AIS users worldwide [Kin18]. Regardless of the large user base of GNSS and AIS, security has never been a high priority for these trust-based systems. Messages that are sent between entities in both the systems are sent in the clear with neither authentication nor encryption and have been known for a long time to be the reason behind why the systems are vulnerable to spoofing attacks. However, the European Union announced in 2017 [Age17] that their Satellite system, Galileo, is going to offer a commercial service that will be initiated in 2020 where encryption is enabled for a fee.

The issue regarding lack of security and the unwillingness of change within GNSS and AIS is the key motivation of this project. The project will investigate the feasibility of attacks on both GNSS and AIS, and determine what kind of knowledge, equipment, and cost that are necessary to launch such attacks. In addition, in-depth interviews will be carried out to explore what kind of mechanisms that are used in the maritime industry to mitigate these risks. The interviews will furthermore give an overview of the overall awareness of the current security risks in the field. Lastly, a literature review will also take place, where potential techniques that can withstand attacks on the systems will be investigated.

Responsible professor:	Karin Bernsmed, NTNU
Supervisor:	Karin Bernsmed, NTNU

Abstract

The maritime shipping industry is experiencing a digital transformation that has a significant impact on operations and existing business models. It has resulted in an industry that is getting increasingly more dependent on digital systems to optimize its efficiency. However, as new technology pushes the industry forward and creates new opportunities, new cyber threats emerge.

Today, the Automatic Identification System (AIS) and Global Navigation Satellite Systems (GNSSs) are two core technologies used to increase navigational and situational awareness. The systems have assisted in increasing the overall safety within the maritime industry. However, apparent weaknesses are present within the systems as neither encryption nor authentication mechanisms are enabled by default. This leaves most GNSS and AIS users vulnerable to attacks. As open-source software becomes increasingly more prevalent, the complexity and cost to exploit the vulnerabilities within AIS and GNSS are steadily reduced. Consequently, leaving most users of AIS and GNSS services more vulnerable than ever.

This master thesis presents the necessary equipment and the process that needs to be conducted to exploit the underlying weaknesses within AIS and GNSS. We conducted two experiments, one for each of the two technologies. The experiments helped identify the simplicity and effort needed to initiate AIS- and GNSS-based attacks. Moreover, we determined the costs associated with initiating such attacks by using the Resource Cost Estimate Model, which is a model based on the Intrusion kill Chain. The model assisted in further identifying the steps AIS- and GNSS-based attacks need to undergo and helped determine the associated cost at each step of the attack. Furthermore, we conducted eight interviews to investigate whether deck officers, maritime pilots, and maritime traffic leaders are aware of the underlying weaknesses within the technologies. The interviewees also outlined the current countermeasures that are set in place to reduce the impact of potential attacks. However, we discovered that these countermeasures are not adequate in sufficiently mitigating today's risks. Lastly, we conducted a literature study that sheds light on techniques that can thwart AIS- and GNSS-based attacks.

Sammendrag

Den maritime skipsfartsindustrien gjennomgår en digitaliseringsprosess som har betydelig innvirkning på drift og eksisterende forretningsmodeller. Dette har resultert i en bransje som blir stadig mer avhengig av digitale systemer for å optimalisere effektiviteten. Når ny teknologi fører industrien fremover og skaper nye muligheter, dukker det imidlertid opp nye cybertrusler.

I dag er Automatic Identification System (AIS) og Global Navigation Satellite System (GNSS) to kjerneteknologier som brukes til å øke navigasjons- og situasjonsbevissthet. Systemene har bidratt til å øke den generelle sikkerheten innad i den maritime industrien. Til tross for dette er det tydelige svakheter i systemene, da verken krypterings- eller autentiseringsmekanismer er til stede. Dette resulterer i at de fleste brukere av GNSS og AIS er sårbare for angrep. Ettersom open-source programvare blir stadig mer utbredt, reduseres kompleksiteten og kostnadene for å utnytte sårbarhetene innen AIS og GNSS jevnlig. Dette resulterer i at de fleste brukere av AIS og GNSS tjenester er mer utsatt enn noen gang.

Denne masteroppgaven presenterer nødvendig utstyr og prosessen som må gjennomføres for å utnytte de underliggende svakhetene i AIS og GNSS. Vi gjennomførte to eksperimenter, ett for hver av teknologiene. Eksperimentene bidro til å identifisere vanskelighetsgraden og innsatsen som er nødvendig for å initiere i gang AIS- og GNSS-baserte angrep. Videre estimerte vi kostnadene forbundet med å sette i gang slike angrep ved å bruke en modell kjent som ”the Resource Cost Estimate Model”, som er en modell basert på ”the Intrusion Kill Chain”. Modellen bidro til å ytterligere identifisere trinnene AIS - og GNSS-baserte angrep må gjennomgå og bidro til å bestemme de tilhørende kostnadene på hvert trinn i angrepet. Videre har vi gjennomført åtte intervjuer for å undersøke om dekksoffiserer, maritime piloter og sjøtrafikkledere er kjent med de underliggende svakhetene teknologiene har. Intervjuobjektene presenterte også mottiltak som er satt i verk for å redusere effekten av potensielle angrep. Vi oppdaget imidlertid at disse mottiltakene ikke er tilstrekkelige til å betydelig redusere dagens risiko. Til slutt gjennomførte vi en litteraturstudie som belyser teknikker som kan hindre AIS- og GNSS-baserte angrep.

Preface

This master thesis was written during the spring of 2020 and concluded our 5-year MSc degree in Communication Technology and Digital Security at Norwegian University of Science and Technology (NTNU). The thesis was developed and written under the supervision of Karin Bernsmed from the Department of Information Security and Communication Technology at Norwegian University of Science and Technology (NTNU).

We want to thank Karin Bernsmed for the guidance and the feedback she gave during this thesis. Additionally, due to her connections in the maritime sector, Bernsmed held a key role in the identification of suitable participants for the interviews.

We would also like to thank Nina Henriette Walde for helping us to get in contact with several deck officers. The deck officers were later interviewed, and the information given was a key part of the findings obtained during the master thesis.

Aleksander Walde & Einar Gaustad Hanus
Trondheim, 15th of June 2020

Contents

List of Figures

Listings

List of Tables

List of Acronyms

2/O Second Mate.

ADC Analog to Digital Converter.

AGC Automatic Gain Control.

AIS Automatic Identification System.

APT Advanced Persistent Threat.

AtoN Aids to Navigation.

BDS BeiDou Navigation Satellite System.

C/O Chief Mate.

CA Certificate Authority.

CNR Carrier-to-Noise Ratio.

CPA Closest Point of Approach.

DDoS Distributed Denial of Service.

DoS Denial of Service.

EAIS Encrypted AIS.

ECDIS Electronic Chart Display and Information System.

ECEF Earth-centered Earth-fixed.

ENISA European Union Agency for Cybersecurity.

ETA Estimated Time of Arrival.

EU European Union.

FFT Fast Fourier Transform.

FTP File Transfer Protocol.

GLONASS Globalnaya Navigazionnaya Sputnikovaya Sistema.

GNSS Global Navigation Satellite System.

GPS Global Navigation System.

GRC GNU Radio Companion.

GSA European Global Navigation Satellite Systems Agency.

GUI Graphical User Interface.

IALA International Association of Marine Aids to Navigation and Lighthouse Authority.

ICS International Chamber of Shipping.

ICT Information and Communications Technology.

IMO International Maritime Organization.

INS Information Service.

IP Internet Protocol.

mIBC Maritime Certificate-less Identity-Based Public Key Cryptography Infrastructure.

MMSI Maritime Mobile Service Identity.

NAS Navigation Assistance Service.

National-mIBC-PKG National mIBC Private Key Generator.

NCA Norwegian Coastal Administration.

NTNU Norwegian University of Science and Technology.

OpenCPN Open Chart Plotter Navigator.

PEC Pilot Exemption Certificate.

PNT Positioning, Navigation, and Timing.

PPU Portable Pilot Unit.

RF Radio Frequency.

SAR Search and Rescue.

SART Search And Rescue Transmitter.

SCG Swedish Coast Guard.

SDR Software-Defined Radio.

SMA Swedish Maritime Administration.

SNR Signal-to-Noise Ratio.

SOLAS Safety of Life at Sea.

SSNN SafeSeaNet Norway.

STCW International Convention on Standards of Training, Certification and Watch-keeping for Seafarers.

SWIG Simplified Wrapper and Interface Generator.

TDMA Time-Division Multiple Access.

ToA Time of Arrival.

TOS Traffic Organisation.

TTP Trusted Third Party.

UHD USRP Hardware Driver.

USRP Universal Software Radio Peripheral.

VHF Very High Frequency.

VIP Very Important Person.

VM Virtual Machine.

VTS Vessel Traffic Service.

Chapter 1
Introduction

1.1 Motivation

The global shipping industry is a $183.3 billion industry and transport an estimated 90% of world trade [TJ18], which makes the industry a critical function of society and a vital asset for the global economy. Modern vessels are today dependant on digital systems for purposes such as engine control, cargo control, and navigation. As it can be seen in other economic sectors, the maritime sector and its activities increasingly rely on Information and Communications Technology (ICT) to optimize its operations. The ever-increasing digitalization trend in the maritime industry has lead to the implementation of electronic systems such as the Global Navigation Satellite System (GNSS) and the Automatic Identification System (AIS) to increase navigational and situational awareness further. However, as the dependency of electronic systems increase, new potential attack vectors disrupting maritime operations emerge. Furthermore, cybersecurity in digital systems used in navigation and collision avoidance such as GNSS and AIS is not only critical for the sake of data protection, but is also affecting the safety of the vessel and the crew onboard. One would, therefore, assume that security was a top priority when implementing such systems. However, this seems not to be the case.

The number of cyber-related incidents within the maritime industry has steadily increased during the last decade. In 2017, the Danish conglomerate Maersk was attacked by the NotPetya malware, which caused their operations to be disrupted for eighth days resulting in a $250-300 million loss [CDQ+19]. Hackers are becoming increasingly aware of cyber-vulnerabilities within the maritime industry, and existing risk assessment tools do not sufficiently represent the unique nature of maritime cyber threats [TJ19].

Based on the statistical data presented by the International Chamber of Shipping (ICS), the global seaborne trade is expected to grow exponentially in the years to come [BYK18]. The increasing traffic leads to difficulties in terms of navigation in coastal

and crowded areas where several vessels are sailing or fishing. The international seaborne traffic is globally dense, but some locations such as the Malacca Strait and the Suez Canal contain particular dense traffic. These respective locations have yearly approximately 50,000 and 20,000 passing vessels, respectively [INR+16].

Accidents such as collisions can result in economic loss, severe damage to the environment, and loss of human lives. Sea surveillance is, therefore, an essential topic in the maritime industry. Consequently, there have been developed several electronic systems to increase the security and safety of navigation at sea. One of these commonly used systems is AIS, which allows a vessel to locate every other AIS device within its radio range. The possibility to identify vessels in the near vicinity increases the situational awareness of the operators of a vessel. It also reduces the likelihood of dangerous situations occurring, as precautions can be taken in advance.

The positional services AIS offers are tightly connected to GNSSs, as the positional data that are transmitted by AIS are obtained by a GNSS. However, both GNSSs and AIS have fundamental underlying weaknesses. Neither of the technologies offers encryption nor any mechanism to ensure the authenticity of the signals by default. Thus, almost all applications and services that use GNSSs and AIS data are vulnerable as no cryptographic protection mechanism is set in place. As a response to the vulnerabilities, a wide range of papers proposing countermeasures have been published during the last two decades. However, the process to mitigate the vulnerabilities has been slow so far, and currently, few measures have been developed, leaving most GNSS and AIS equipment vulnerable.

1.2 Research Questions

AIS- and GNSS-based attacks are not new phenomena, and several papers have been published demonstrating such attacks. However, the papers focus, for the most part, on demonstrating that such attacks are possible and do not give emphasis to the complexity and cost. This master thesis aims to fill this gap and thus investigate the complexity and cost that are associated with such attacks. In order to identify the severity of the attacks, interviews have been conducted with individuals using navigation equipment daily.

Based on these topics, six research questions have been formed and will be addressed.

- **RQ1:** What kind of resources are necessary to launch successful AIS- and GNSS-based attacks in the maritime sector, and how feasible are such attacks?
- **RQ2:** How critical are AIS and GNSS services for the industry?
- **RQ3:** How well prepared is the industry to handle incidents affecting navigational equipment dependent on AIS and GNSS services?
- **RQ4:** What could be the potential outcome of AIS- and GNSS-based attacks?
- **RQ5:** Based on the estimated cost and the potential outcomes of such attacks, which cyber threat agent groups pose the highest threat to the industry?
- **RQ6:** Which techniques could be implemented to thwart the attacks?

1.3 Limitations

This section highlights the most important limitations that were encountered during the master thesis.

The Norwegian government chose to close down a substantial part of the Norwegian society on the 12th of March 2020 due to the Covid-19 pandemic. Additionally, a wide range of restrictions were made to stop the spread of the virus. The restrictions impacted the planned interviews, as they had to be rescheduled. Initially, several interviews were planned to be conducted in-person, allowing us to observe the equipment they were using and to create a more relaxed and pleasant atmosphere. Due to the extraordinary situation, this was not possible, and only one of the interviewees was willing to meet in person. Thus, the rest of the interviews had to be conducted via Skype or phone, which likely reduced the overall quality of the interviews.

A commercially available AIS transceiver would be preferable when the AIS-based attacks were executed, as it would ensure that the attacks were successful on commercially available devices. However, an Software-Defined Radio (SDR) had to be used to receive the forged AIS messages as a commercial AIS transceiver was not accessible.

1.4 Outline

The structure of the master thesis is as follows:

- **Chapter 2** (Background and related work): presents necessary background information and discusses related work that has been conducted on the topic.
- **Chapter 3** (Methodology): describes the methods that have been used to obtain the results presented in the thesis.
- **Chapter 4** (GPS experiment): presents equipment and steps necessary to execute Global Navigation System (GPS) spoofing attacks.
- **Chapter 5** (AIS experiment): presents equipment and steps necessary to execute a range of AIS-based attacks
- **Chapter 6** (Resource cost estimate): estimates the cost of GNSS spoofing and AIS-based attacks.
- **Chapter 7** (Interview findings): presents the findings that were obtained from the interviewees.
- **Chapter 8** (Discussion): discusses the research questions in relation to the findings.
- **Chapter 9** (Conclusion and Future Work): concludes the thesis and proposes further work.

Chapter 2
Background and related work

The following chapter will present the background necessary to grasp the fundamental parts of how a GNSS and AIS function. Furthermore, the underlying weaknesses of the systems will be addressed, and potential countermeasures will be explored.

2.1 Global Navigation Satellite System (GNSS)

GNSS is an umbrella term used to cover satellite constellations that provide Positioning, Navigation, and Timing (PNT) services. The term includes satellite constellations that provide these services both on a regional or a global basis. The term can also refer to augmentation services that are used to improve attributes, such as accuracy, reliability, and availability. There are currently three satellite constellations that can provide GNSS services on a global scale, but this number will increase to four within 2020 [GOVb]. The four satellite constellations are as follows:

The GPS, known initially as NAVSTAR GPS, is a global GNSS owned by the United States government and operated by the United States Space Force. GPS was originally intended for military use only, but civilians were after a while given access to the primary services that the system provided. The Department of Defense initiated the GPS project in 1973, and had 24 fully operational satellites in 1993 [NAS12].

The global GNSS, known as Globalnaya Navigazionnaya Sputnikovaya Sistema (GLONASS), is operated by the Russian Federation. Flight tests of the system were started in 1982, and the system was formally declared operational in 1993, with a fully operational constellation of 24 satellites in 1995 [GLO].

Galileo is a global GNSS that was operational in 2016 and was created by the European Union (EU) through the European Global Navigation Satellite Systems Agency (GSA). The system is scheduled to be completed in 2020 and will offer, among

other, commercial services that enable encryption and highly accurate poisoning for a fee [Age17].

The BeiDou Navigation Satellite System (BDS) is the second-generation of the Chinese satellite navigation system. The system is currently expanding so that it can provide its users with global coverage. The expansion is scheduled to be completed within 2020, where 35 satellites will be in orbit to provide the global coverage [ge11].

2.1.1 Fundamentals

GNSS satellites constantly transmit signals containing information such as timestamp and the orbital position of the transmitting satellite. When a user of the system receives a signal, the user calculates the transmission distance. The distance is calculated from the transmission speed, which is the speed of light, and the transmission time. However, it is important to note that GNSS signals hold an important characteristic known as line-of-sight propagation, which means that the signals travel in a straight line, and because of this characteristic, GNSS receivers are only able to obtain signals from satellites that are within the line-of-sight from the receiver.

The position of a GNSS device can be determined by combining the signals from multiple satellites. A device requires to simultaneously receive signals from no less than four different satellites to derive a precise position of the device. Locking onto more satellites will increase the accuracy of the location derived, but is not strictly necessary. Three of the signals are used to determine the longitude, latitude, and altitude by using trilateration, which is the three dimensional equivalent of triangulation. However, the clock inside GNSS receivers are not nearly as accurate as those that are within the satellites, which, if not accounted for, would result in an inaccurate position. Consequently, a fourth signal is necessary to identify the offset between the clock in the receiver and clock in the satellite.

2.1.2 GNSS Segments

GNSS satellite systems consist of three main segments: The space segment, the control segment, and the user segment as shown in Figure 2.1 [Jef10].

The space segment refers to a set of satellites known as a constellation, which is used by a GNSS. Each satellite in the constellation sends out information regarding its identity, its time, orbit, and the status.

The control segment consists of ground-based stations, which are used for purposes such as monitoring and updating of satellite information. A GNSS control segment consist of three components, a data uploading station, a master control station, and a monitoring station.

The user segment consists of components that receive and process signals from GNSS satellites to determine the position of the component or for timing purposes. The main elements of the user segment are the antennas and the receivers. GNSS antennas receive the signals from satellites and forward these to the receivers. After obtaining the signals from the antenna, the receiver calculates the position and time, which then can be used by a wide range of applications. It is also important to note that GNSS receivers can be designed to use signals from several GNSS constellations. Resulting in improved coverage and accuracy, as more satellites are available at the same time.

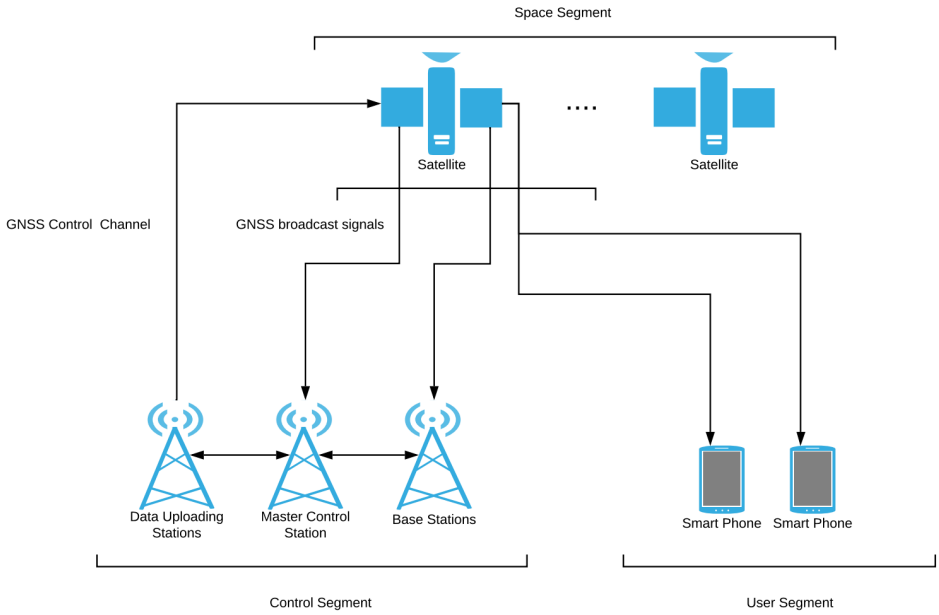


Figure 2.1: GNSS architecture (inpsired by [Jef10])

2.1.3 Vulnerabilities in GNSS

A GNSS consists of several segments which are not necessarily vulnerable to the same type of errors or attacks. This project is, however, only interested in the user segment and vulnerabilities related to it, as this segment is affected by most attacks. Consequently, this section will focus on vulnerabilities that affects the user segment.

Interference

The impact of interference on GNSS receivers varies depending on factors such as strength and type of the interference. Interference can increase the receiver in-band noise and decrease the receiver Signal-to-Noise Ratio (SNR). A receiver experiencing interference will display a lower Carrier-to-Noise Ratio (CNR) and obtain noisier GNSS measurements. Resulting in degraded positioning and timing performance, and can in severe cases, resulting in the inability to determine position and time. GNSS receivers are also designed to be very sensitive so that they are able to recover GNSS signals sent by the satellites, as these signals can have a signal power around -120dBm to -130dBm when received by the receiver [Nov15] [GPS95]. As a consequence, even a small interference can degrade the GNSS service.

Unintentional interference

Unintentional interference can arise from a number of potential sources from both in-band and out-of-band emitters, such as interference from Very High Frequency (VHF) communication, television signals, certain radars, mobile satellite communication, and military systems. Although sources of interference can occur in both in-band and out-of-band emitters, out-of-band emitters are more often the reason behind unintentional interference due to spectrum regulations.

Intentional interference

Intentional interference is the act where an adversary knowingly interference with legitimate signals to achieve a particular goal. In the case of GNSS signals, intentional interference can be divided into two subcategories: *jamming* and *spoofing*.

Jamming is the act of deliberately transmitting signals at GNSS frequencies with a relatively high signal power as compared to legitimate GNSS signals. As a consequence, GNSS receivers will not be able to retrieve legitimate GNSS signals. The goal of jamming is to deny any kind of service to the targeted GNSS receiver. Despite the potential impact of jamming, adversaries with little to no knowledge can successfully perform jamming by using GNSS jamming equipment. Such equipment is available for anyone and costs as little as 30 euros. In 2013, The Guardian reported a problem where thousands of people were using cheap jamming equipment, stopping tracking systems detecting stolen cars [Art13].

Spoofing is the deliberate act were an adversary transmits illegitimate PNT data to a GNSS receiver. If done successfully, the receiver interprets the illegitimate PNT as legitimate. Spoofing is possible because signals transmitted from the satellites are neither encrypted nor authenticated. However, not all GNSS services send signals unencrypted, among others, GPS offers cryptographic signal protection for signals that are used by the military [Age11]. This service is, however, only for military purposes, and similar services are not yet publicly available. Nevertheless, by 2020, the EU will offer a commercial service where encryption could be enabled for a fee [Age17]. This commercial service could, as a result, at least prevent some types of spoofing attacks from being successfully initiated.

Humphreys et al. [HLP+08] classifies three types of spoofing attacks: *simplistic attacks*, *intermediate attacks*, and *sophisticated attacks*.

Simplistic attacks refers to attacks composed of a GNSS signal generator broadcasting spoofed signals, and a transmitting antenna. A simplistic attack requires no knowledge of the targets PNT. The attack can be easily detected due to the inconsistency in frequency, phase, code, and data message, which can be monitored by the target. Humphreys et al. assumed that simplistic attacks most likely are executed by using signal generators implemented in hardware such as GNSS simulators. A device typically used for laboratory testing purposes. According to Humphreys et al., a simulator could cost up to $ 400k or be rented for less than $ 1000 a week. However, these price estimates are likely no longer accurate as the paper was released in 2008.

Intermediate spoofing attacks have knowledge related to the conditions in which the signals are sent. An intermediate spoofing attack is carried out by using a GNSS receiver positioned relatively close to the target and a signal generator. The receiver tracks the satellite signals to precisely determine important parameters that are obtained by the victim's receiver, such as the signal strength of the legitimate signals. The signal generator uses these parameters to forge fake signals with similar features as the real signals. As a result, the signals sent from the adversary seem more legitimate compared to a simplistic attack.

A **sophisticated attack** is similar to an intermediate attack. However, sophisticated attacks use several coordinated spoofers to emulate illegitimate signals. As a result, a victim is prevented from detecting that the illegitimate signals originated from only one location. If all the signals originate from one location, the victim would have a reason for concern, as it is likely that the victim is under a spoofing attack.

2.1.4 Countermeasures

There have been proposed a wide range of countermeasures and detection techniques to prevent both spoofing and jamming attacks. This section defines the three main classes, proposed by Psiaki et al., that can be used to thwart the effectiveness of spoofing attacks. The first class utilizes cryptographic solutions as a countermeasure. The second class utilizes a protection mechanism based on signal-distortion detection. Lastly, the third class utilizes a protection mechanism based on direction-of-arrival sensing [PH16b].

Cryptography

Cryptographic protocols and primitives may be utilized to make it challenging for adversaries to interpret and reproduce the signals generated by a GNSS. However, depending on the chosen implementation strategy, the result would differ with regards to performance and the security level achieved.

Psiaki et al. propose several techniques in their paper, which could be implemented to increase the overall security of the system [PH16a]. One of the proposed techniques to thwart spoofing attacks is a strategy based on symmetric cryptography. Satellites would encrypt the signals, and decryption keys would be distributed among the users of a GNSS. The encryption would make it harder for adversaries to forge signals, but replay attacks would still be possible, as no forward secrecy is applied. However, if an adversary can obtain the symmetric key distributed among the users, forged signals can be crafted.

An alternative technique is to store and record encrypted GNSS signals on the GNSS receiver, without knowing the decryption key [PH16a]. After a certain period, the satellite would broadcast the decryption key, which is digitally signed by the satellite. The user could verify the decryption key by inspecting the signature and then decrypt the stored signals. However, this strategy would require quite large changes in regards to how the receiver processes the signals, and how signals are transmitted by the satellites. In addition, positional updates would be slightly delayed rather than instantaneously.

Signal-distortion detection

Signal-distortion detection is a class of defense techniques that search for irregularities related to distortion and disruption of GNSS signals. The most straightforward detection technique, according to Psiaki et al., searches for sudden changes in the received carrier amplitude, beat carrier phase, or code phase that seems unreasonable [PH16a]. These parameters typically change at the start of an attack and are therefore of particular interest when developing a defense. By adding additional hardware that

can process the signals to a greater extent, irregularities and unnatural features can be more easily detected and alert users.

Direction-of-arrival sensing

Direction-of-arrival sensing is a technique that exploits how adversaries are only able to transmit signals from one location at the time. Authentic GNSS signals, on the other hand, arrive from several directions because the satellites sending the signals have different locations. As a consequence, if the victim can detect the direction where the signals are transmitted from, a spoofing attack would be easily detectable.

Psiaki et al. demonstrated this defense technique by using a software-based system with two antennas that applied the principles of interferometry [PH16b]. Interferometry is the umbrella term used for techniques where waves are superimposed, causing interference. The interference is then used to extract information regarding the signals. In the case of Psiaki et al., the system monitors how the carrier phase varies from the first to the second antenna to determine the variation of the signal. By determining the variation between the carrier phase for signals obtained by the two antennas, the system can conclude whether or not the signals are originating from the same location. If the variations between the signals sent by two satellites are significant, it is likely that the signals are originating from several locations and therefore are not spoofed. However, if the variation is small, the signals are likely to come from a spoofer.

Initially, off-line computing was required to identify whether the GNSS receiver was under attack and detection in real-time was not possible. However, in 2014 this system was improved upon, and only a 6-second delay was necessary to identify a potential attack [PH16b].

2.1.5 Related Work

GNSS jamming and spoofing have been an issue for over two decades. Few adjustments have been made towards the systems to increase security and reduce the impact of such attacks. The lack of security motivated researchers to research the topic and have resulted in a wide range of detection and countermeasures. This section will, however, not provide a comprehensive review of the countermeasures and detection techniques that have been proposed, as it would be too extensive. This section will instead highlight some of the countermeasures and detection techniques that were considered the most interesting.

GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)

In 2012, Akos released a paper where spoofing detection was possible by utilizing a component most GPS receiver use to minimize digitization loss [Ako12].

GPS receivers that utilize multibit sampling relies on a component known as the Automatic Gain Control (AGC). The AGC serve as a variable gain amplifier to adjust the power level of incoming signals. The AGC uses a variable gain to maintain a suitable output, regardless of variations of the input. The AGC is positioned between the analog portion and the Analog to Digital Converter (ADC) within the receiver. The AGC optimizes the gain to minimize the digitization loss that occurs during the digitization process. Typically, the GPS band is interference-free as there are restrictions and regulations regarding emission in and close to the band. Hence, the AGC gain will remain stable since thermal noise is almost exclusively the only dependent factor on the AGC gain and is a factor that has minimal fluctuation. Thus, in case of an event where interference of some sort occurs, the AGC gain will rapidly change and can be used to identify potential interference. However, the sensitivity level is essential when using such a detection technique, as an increase in sensitivity may increase the false positives.

GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation

Broumandan et al. proposes a GNSS spoofing detection technique by using a single antenna based on signal spatial correlation. Signal spatial correlation is a technique that investigates the correlation of the average gain and angle of arrival of a signal [BJJD+12]. The researchers assume that most adversaries performing spoofing have one major weakness in common. The adversaries transmit the signals from a single source. As a consequence, the adversaries are forced to transmit highly correlated GNSS signals simultaneously to be able to present seemingly legitimate GNSS signals to the victim. Consequently, the researchers propose a detection scheme that exploits this weakness to identify potential illegitimate signals.

A Key Management Architecture for GNSS Open Service Navigation Message Authentication

Caparra et al. proposes a three-layered key management scheme as a way to ensure navigation message authenticity [CCSL17]. The layered structure gives the key management scheme much flexibility when it comes to updating and revocation of keys within the system. The top layer keys, known as the root keys, ensure the integrity of the keys at both the underlying layers. The root-level consist of long-term private/public key pair which are bound to a Certificate Authority (CA). The underlying level, known as level two, consists of medium-term private/public key pairs. The key pairs are used to sign crucial messages such as updating or in case of revocation of keys. The lowest level, known as level one, consists of short-term private/public key pairs and are the keys used to signs navigation messages to ensure authenticity.

To utilize the key management scheme, the receiver needs to pre-install a set of information. First and foremost, the public key associated with the CA needs to be installed by the manufacturer. The public key is a necessary component to ensure the authenticity of layer two and layer one keys. Secondly, system configurations and other key material can either be provided by the manufacturer or extracted by utilizing a secure internet connection.

One crucial feature of the scheme is its robustness against key compromise, as the keys at the second and first layers can be renewed if a compromise happened. Caparra proposes that level one public keys should be broadcasted alongside a level two signature when new level one public keys are required. However, the bandwidth in the case of GNSS is a scarce resource, and frequent transmission may be too costly for the system. Due to this, the researchers propose that a batch of level one public keys may be stored at the receiver. Consequently, the receivers will be able to act autonomously for a certain period, and the importance of frequent transmissions decreases. Caparra et al. do not specify how level two public keys are updated other than that it should go through an aided channel.

2.1.6 GNSS in the maritime sector

The service offered by GNSSs holds a key role in how navigation is utilized within the maritime sector. Positional information that is obtained by GNSSs is vital for shipboard technologies such as AIS and Electronic Chart Display and Information System (ECDIS), which are used to navigate safely at sea. Not being able to pinpoint a vessel's position precisely can, in the worst case, be the cause of disaster.

GNSS services also play an important role in the maritime traffic control and for vessel route planning. Positional information is continuously received by the

GNSS receiver onboard vessels. The information is then broadcasted through AIS and received by other vessels, base stations, and satellites. Subsequently, by using the broadcasted positional information, an overview of the vessel traffic can be made. The traffic overview is essential for optimal operation for both maritime traffic control centers and vessels, as the data assist in making favorable decisions. Consequently, vessels have the opportunity to decide routes depending on traffic, avoiding undesirable and dangerous situations occur. In the case of maritime traffic control, to give helpful advice, a good situational awareness is required and is partly obtained as a consequence of the broadcasted positional data.

2.2 Automatic Identification System (AIS)

AIS was developed to provide an automatic exchange of information between vessels sailing in open waters and between vessels and stations located at the shore. Today, the system is used by the vast majority of the global maritime shipping industry. Since 2002, AIS has been mandatory equipment for vessels having a gross tonnage of at least 300 [SOL]. AIS is an important tool used for traffic management, collision avoidance, Search and Rescue (SAR) operations, and aids in navigation [BPW14]. AIS is not solely used onboard vessels, several different AIS devices, also known as stations, such as AIS base stations, AIS Aids to Navigations (AtoNs), and Search And Rescue Transmitter (SART) also uses AIS for additional purposes. Every station is identified by a unique code known as Maritime Mobile Service Identity (MMSI) [No16].

The exchanged information can be classified as static, dynamic, voyage related, and safety-related. Static information consists of data, such as MMSI, length, and type of vessel. Dynamic information includes the course, position, speed, rate of turn, and the navigational status of the vessel. Voyage related information consists of data, such as cargo type, destination, and Estimated Time of Arrival (ETA). Safety-related information can consist of weather reports and Search And Rescue Transmitter (SART) messages [GK19].

A total of 27 different application-specific messages are currently available in AIS, as defined in ITU 1371-5 [IR14]. However, the system is capable of increasing this amount to a total of 64 different application-specific messages if deemed necessary in the future. The currently available messages are specified in appendix B.

AIS transceivers automatically broadcast information at fixed intervals. The navigational status data of a vessel is transmitted every 2 to 180 seconds, depending on the vessel's activity. In addition, voyage related data is broadcasted every 6 minutes. These signals are received by AIS transceivers installed on other vessels or by land-based systems. [Age]. Over the last couple of years, AIS collection networks have been developed to provide global vessel tracking services. Websites such as *marinetraffic.com* and *vesselfinder.com* enables free access to databases containing vessel names and their corresponding real-time location anywhere in the world, as shown in figure 2.2.

The system operates over the VHF maritime mobile band to receive and transmit information using the dedicated frequencies 161.975Mhz and 162.025Mhz. Although only one radio channel is necessary, AIS uses two channels to transmit and receive to avoid interference [AIS].

POSITION & VOYAGE DATA	
AIS Type	Cargo ship
Flag	Hong Kong
Destination	JORF LASFAR
ETA	May 17, 11:00
IMO / MMSI	9602966 / 477317200
Callsign	VRIE2
Length / Beam	190 / 32 m
Current draught	11.3 m
Course / Speed	239.0° / 11.7 kn
Coordinates	49.44102 N/4.4483 W
Status	-
Position received	19 mins ago

Figure 2.2: Information on a arbitrary vessel from www.vesselfinder.com.

2.2.1 NCA AIS chain

The Norwegian Coastal Administration (NCA) operates what is known as the NCA AIS chain. In 2013, the chain consisted of 44 land-based base stations along the Norwegian coast [Bar13]. The chain is used for distribution and collection of AIS data transmitted nearby the Norwegian coast. The AIS chain covers the baseline, which is the boundary line that dictates where a state has maritime sovereignty and jurisdiction. In addition, another 40-60 nautical further out to sea. Furthermore, the NCA also has access to four satellites (AISSat-1, AISSat-2, NorSat-1, and NorSat-2). The access increases the coverage by relaying the AIS information they obtain. The data obtained by the land-based stations and the satellites are then made available to various public authorities in Norway through a web-based service.

An example of a user of this service is the Norwegian Coastal Administration's traffic control centers. They combine data received from the AIS chain with data from the SafeSeaNet Norway (SSNN) massaging system to get a situational overview of the vessel traffic in Norwegian waters. SSNN is an internet-based reporting system where vessels can provide notifications such as port arrival and port departure notifications to Norwegian governmental authorities [Adm11b].

2.2.2 Vulnerabilities in AIS

AIS is known to be vulnerable to a handful of attacks. The following attacks described in this section were conducted by Trend Micro in 2014 while performing a security evaluation of AIS [BPW14]. The attacks are classified into two groups, either as software-based attacks or as Radio Frequency (RF)-based attacks. Software-based attacks target online services and do not use any types of radios to forge illegitimate signals. RF-based attacks, on the other hand, forge illegitimate signals by using SDRs and have the ability to target particular vessels, unlike software-based attacks.

Closest Point of Approach (CPA)

As previously mentioned, AIS provides important information such as location, course, and identification of vessels within the RF coverage, to aid in collision avoidance. Collision avoidance is an important feature of AIS, and it offers an automatic response when a collision is detected or expected. Closest Point of Approach (CPA) is an estimated point between two objects, of which at least one is in motion. CPA can be configured to alert the captain when a potential collision is detected.

The CPA algorithm, as illustrated in Figure 2.3, allows deck officers to estimate the remaining time and distance before a potential collision, assuming that both vessels are sailing at fixed courses and speeds. T_{CPA} represents the estimated time to CPA, while D_{CPA} represents the distance between the vessels before they reach the CPA. It is possible to configure a CPA alarm to alert the deck officers when one of these parameters goes below a pre-configured threshold [BPW14]. In a CPA spoofing attack, the goal is faking a possible collision with another vessel. The attack can trigger a CPA alarm that can steer the vessel off course and into dangerous waters.

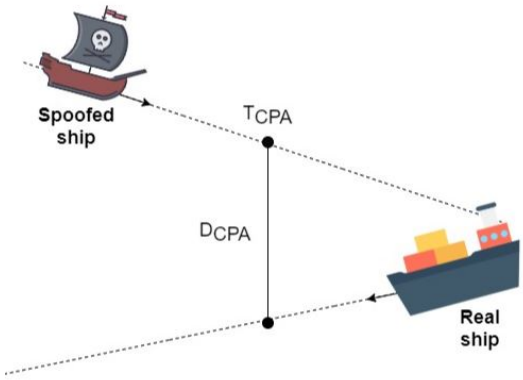


Figure 2.3: Closest point of approach algorithm (inspired by [BPW14]).

AIS-SART spoofing

AIS is also commonly used in SAR operations. SART is a waterproof radio device that assists in locating a vessel or person in an emergency. The device uses a radio-beacon to broadcast the position once every minute. The goal of AIS-SART spoofing attacks is to generate false distress signals to simulate a person in an emergency [BPW14]. The coordinates in the distress signal are crafted by the attacker, which allows the attacker to lure vessels into dangerous waters. AIS transceivers are required to alert the deck officers when receiving a distress signal. Vessels are required by law to engage in SAR operations due to the SAR convention from 1979 [Man86].

Vessel spoofing

The goal of a vessel spoofing attack is to create a valid but non-existing vessel appearing on the surveillance screens. The process involves assigning valid static information such as name, MMSI, vessel type, and dimensions to a non-existing vessel. The spoofed vessel will also be assigned dynamic information such as speed, course, status, destination, and position [BPW14]. An attacker can perform several different malicious acts with vessel spoofing. For instance, an attacker can spoof the location of a warship onto waters that are a part of an international conflict causing political tensions.

AtoN spoofing

AtoNs are used to assist in vessel traffic management along common vessel routes and harbors. They are also used to warn about bad weather, low tides, and reefs. Common types of AtoNs include but are not limited to lighthouse, buoys, and Vessel Traffic Services (VTSs). Attackers can modify information provided by AtoNs installed by authorities for vessel support and monitoring. The goal of AtoN spoofing is to generate fake information to lure target vessels into making the wrong maneuvering decisions. An attacker can, for instance, place a fake buoy at a harbor entrance to tamper with traffic management or even lure vessels to navigate in low tide. Since there are different types of existing AtoNs, an attacker can craft several different attack scenarios, as with vessel spoofing [BPW14].

AIS hijacking

The goal of AIS hijacking is to modify any type of information about AIS stations such as speed, course, cargo, country, and type. The attack can be both software-based and radio frequency-based. In a software-based attack of AIS hijacking, an attacker eavesdrops on the communication and can replace it with AIS information of his choice. In radio frequency-based attacks, an attacker sends modified AIS signals

with higher transmission power than legitimate AIS signals. The AIS signals crafted by the attacker will be received instead of legitimate AIS signals [BPW14].

Denial of Service (DoS)

AIS uses Time-Division Multiple Access (TDMA) protocols to enable communication between stations [Age]. Figure 2.4 illustrates the AIS data transmission protocol. Denial of Service (DoS) attacks in AIS can be categorized into the following types:

- **Slot starvation:**
  - In a slot starvation attack, the goal is to reserve all the slots in a frame to prevent other stations within the radio coverage to access free slots. When a legitimate station tries to transmit data, the communication is "blocked" due to the lack of free slots in the frame. This can prevent AIS communication on a large scale.
- **Frequency hopping:**
  - The goal of a frequency hopping attack is impersonating maritime authority to command one or more AIS transceiver to change the frequency that they are currently transmitting on. Receiving stations are obliged to follow instructions they receive from maritime authorities. Rebooting the AIS transceiver does not help because stations can only change the frequency when there is a request from a maritime authority. An attacker can also "program" a desired target region such that when a vessel enters this region, the vessel will change frequency to one chosen by the attacker [BPW14].
- **Timing attacks:**
  - An attacker can also instruct AIS transceivers to delay their transmission times by re-sending commands (replay attack). This results in vessels disappearing from AIS-enabled radars. Attackers are also able to flood the marine traffic by requesting stations such as vessels and VTSs to send AIS information and updates at very high rates [BPW14].

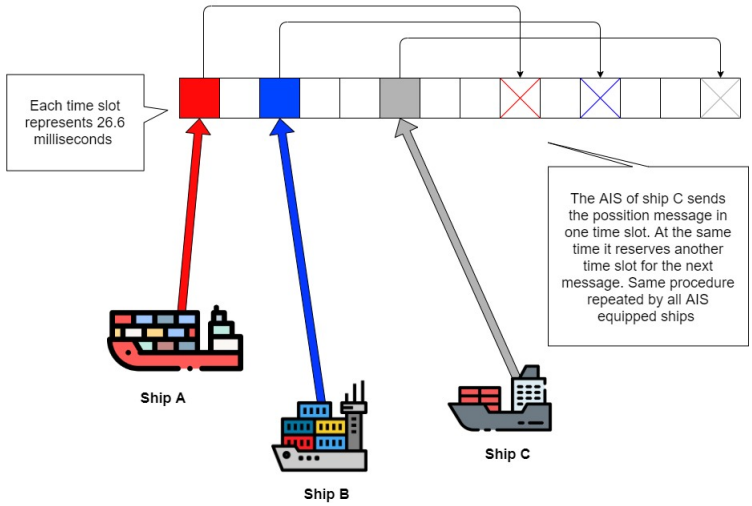


Figure 2.4: AIS data transmission protocol (inspired by [No16])

2.2.3 Countermeasures

As seen in the previous section, AIS is vulnerable to several attacks. This section will present some proposed security enhancements for AIS. Goudossis et al. [GK19] proposes a theoretic solution using a Maritime Certificate-less Identity-Based Public Key Cryptography Infrastructure (mIBC) to secure AIS. Furthermore, some of the exploits introduced by Trend Micro [BPW14] were reproduced in [HLB+15], and a possible solution using IEEE1609.02 certificates was proposed. The solution was verified by running several simulations in a lab environment.

New protocol based on IEEE1609

Hall et al. [HLB+15] propose a three-tiered approach to security with vessel identity verified by certificates assigned by an approving authority. The tiers represent modes with different functionality. A vessel communicates using a pseudonym, a randomized identity based on the certificate that ensures both privacy and authenticity. The pseudonym is created and distributed using the existing IEE1609.2 standard and is a unique identifier for every AIS station. Every AIS station would be issued a certificate by a central authority that ensures the correctness of AIS information such as vessel name, MMSI, destination, etc. This information would not be modifiable by the user.

Tier One In this Tier, vessels operate in a mode called *Navigational Safety Mode*, which is the operating mode by default. In this mode, the vessel is only broadcasting limited navigational data such as location, course, speed, and time of broadcast, as

shown in figure 2.5. Even though this mode only broadcasts limited navigational data, it still offers enough data to preserve the crucial anti-collision feature of AIS. The mode avoids broadcasting private information not necessary for standard operations. The limited broadcasted information ensures both privacy and confidentiality to AIS.

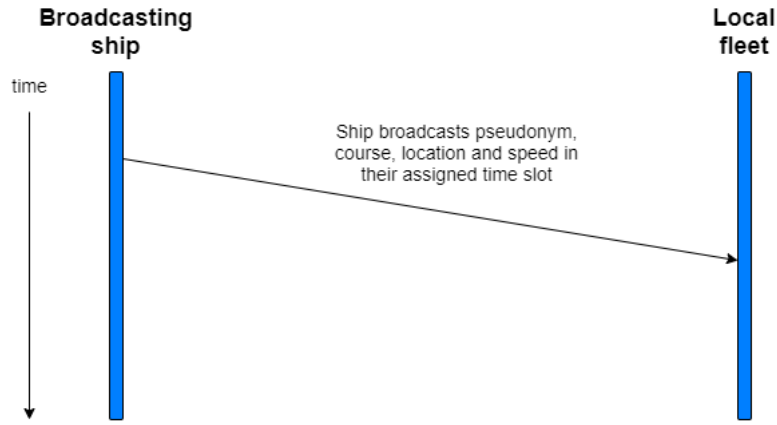


Figure 2.5: AIS data broadcasted in Tier One (inspired by [HLB+15])

Tier Two This Tier contains the feature *Amplified Information Request*, which allows a vessel to query specific information from another vessel, shown in figure 2.6. If the receiving vessel accepts the incoming request, it sends a packet in return containing the amplified information such as the vessel name, for instance. The receiving vessel may, however, not accept the request to send their amplified information. The data transmitted is encrypted by a modified public-key encryption scheme. The pseudonym based encryption ensures that every AIS station is who they claim to be, which again ensures authenticity in the AIS.

Tier Three The final Tier is a *Full Vessel Information Retrieval Broadcast*, which is only accessible by designated security organizations, as shown in figure 2.7. This Tier allows certain users, such as maritime authorities, the ability to obtain every information detail concerning a target vessel. The user can obtain the information without the responding vessel's consent. The exchange of information would, as in Tier Two, be encrypted and authenticated using the user's certificate-validated credentials.

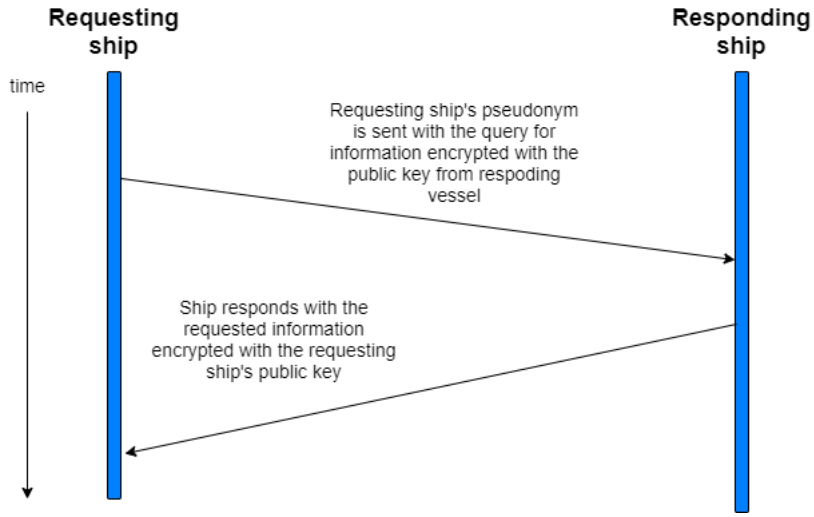


Figure 2.6: AIS data broadcasted in Tier Two (inspired by [HLB+15])

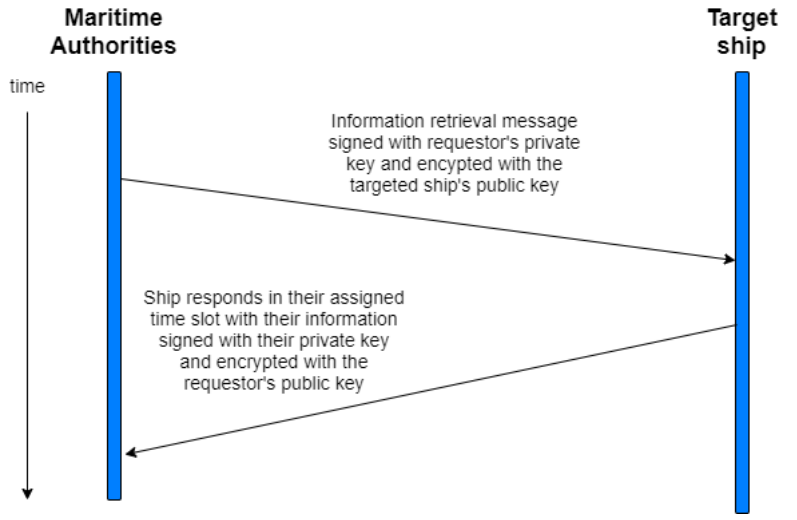


Figure 2.7: AIS data broadcasted in Tier Three (inspired by [HLB+15])

A Maritime Certificate-less Identity-Based Public Key Cryptography Infrastructure (mIBC)

Goudossis et al. [GK19] proposes a mIBC to ensure source authentication, data integrity, privacy-preserving, and encryption in AIS. The public key is a unique identifier for every mIBC station. It is, therefore, no need for Certification Authorities nor certificates. The unique MMSI numbers are used to generate the public keys, and the National Authorities generate the corresponding private keys. To preserve the vessel's privacy, a vessel can send a signed request to its National mIBC Private Key Generator (National-mIBC-PKG) authority requesting a valid pseudonym MMSI. With a valid pseudonym MMSI, the vessel can transmit anonymously over AIS. To keep track of a vessel's true identity National-mIBC-PKG need to store records that bind pseudonym MMSI numbers to the corresponding vessels.

In *insecure sea areas*, AIS navigational data should only be transmitted and received by legitimate vessels. Goudossis et al. proposes on-demand encryption of legitimately broadcasted AIS data. As a consequence, only legitimate vessels can decrypt broadcasted AIS navigational data. The use of encrypted AIS is only available in officially declared *insecure sea areas*. This is due to the difficulties in pre-determining legitimate vessels since they might not also be lawful. Goudossis et al. presume that international maritime authorities such as International Maritime Organization (IMO) and International Association of Marine Aids to Navigation and Lighthouse Authority (IALA), along with national maritime authorities, should have the responsibility to officially declare sea areas as insecure sea areas. It is possible for a Trusted Third Party (TTP) like a military patrol vessel to distinguish between legitimate and suspicious vessels in an insecure sea area, which creates the backbone for encrypted-AIS. The number of vessels passing through an insecure sea area is arbitrary. The AIS data traffic is, therefore, neither pre-agreed nor pre-determined. mIBC is a branch of public-key cryptography, which makes it ideal for one-to-one authentication and encrypted communications without any pre-agreement.

Goudossis et al. [GK19] proposes to use mIBC infrastructure to distribute a symmetric key to the entities wanting to encrypt their communications with a cryptographic algorithm. The keys for the symmetric encryption is generated and distributed by a TTP, and encrypted with the receivers public key. As a result, vessels in an insecure sea area can to broadcast encrypted AIS data as well as decrypt received AIS data. Suspicious vessels will not receive the symmetric key of the encrypted-AIS and will, therefore, not be able to decrypt any of the broadcasted AIS messages in the insecure sea area. Legitimate vessels will, as a consequence, stay hidden from suspicious vessels.

2.2.4 Related work

There has not been published much research regarding security in AIS, which is surprising due to the comprehensive vulnerabilities that exist in the system. In addition to the countermeasures discussed in section 2.2.3, there are limited research regarding securing AIS.

Commercial AIS products offering encrypted AIS communication already exists. However, they can only provide encrypted AIS communication to vessels with the same AIS equipment installed onboard. The U.S Coast Guard uses Encrypted AIS (EAIS) for military and law enforcement purposes [Par14]. EAIS allows their "fleet" of vessels to see each other and, at the same time, stay hidden from vessels outside their "fleet". The vast number of vendors offering a variety of AIS equipment, requires a standardized and practical solution to cope with all the different equipment. Goudossis et al. [GK19] proposes to use a Secure-AIS-Middle-Ware. The middle-ware will process and forward data such as course, speed, location, and cargo to AIS, which broadcast it. Received AIS messages are forwarded to the middle-ware for processing, and the data is then presented for the deck officers.

There have also been very few interviews in the maritime industry regarding AIS. However, in 2006, Andreas Westerberg interviewed key persons in the Swedish Maritime Administration (SMA) and Swedish Coast Guard (SCG) regarding costs and benefits associated with AIS for his master thesis [Wes06]. One of Westerberg's goals was determining if AIS was beneficial for Sweden. Through the interviews, he concluded that AIS indeed was beneficial. The system enhanced the efficiency in Search and Rescue (SAR) operations and assisted the SCG in their surveillance of the Swedish coast.

2.3 Threat Agents

European Union Agency for Cybersecurity (ENISA) publishes yearly reports providing comprehensive reviews of the state of the threat landscape during the previous year. The most recent report was published in early 2019 and reviews the threat landscape of 2018 [SDM+19]. The report identifies the top six threat agent groups and their engagement in the threat landscape. This section discusses the six groups, starting with the most active group during 2018 and ends with the least active group.

Cybercriminals are the most active group and are responsible for over 80% of incidents that occurred during 2018, according to ENISA [SDM+19]. The group is mainly motivated money and is considered to be a group that is well equipped and well funded. Additionally, the actors within the group are assumed to be knowledgeable to a degree where the malicious activity can be completed without ease. Typically these actors aim to steal data or install ransomware as a way to extort money out of the victim. ENISA identified in their report that over 90% of the cyber-attacks involved email [SDM+19], which is a well-suited platform to deliver a malicious payload and to obtain sensitive data.

Insiders are the second most prevalent threat and consist of malicious or negligent insiders. The group is responsible for around 25% of breach incidents that occurred during 2018 [SDM+19]. Motivated by revenge or money, proprietary assets or information are destroyed or delivered to malicious agents. However, not all insiders have malicious intents, some of the agents are just naive or careless, and thus either give away sensitive information or operate in a way that is favorable for the adversary.

Nation States are the third most active group and are driven by economic, political, espionage, and military-based factors. Typically targeting large corporations, the group gain persistent access to the network to steal, change or destroy information. Several international headlines have been made the last couple of years where Nation states have been the accused actors. The maritime industry has not been left alone from these attacks and has been either targeted or affected on several occasions [GPS17] [WB19] [C4A19]. In 2019 the UK-flagged tanker Stena Impro was seized by Iran's Revolutionary Guards for alleged marine violations. Several headlines were afterward made, which stated that it was likely that the GNSS data Stena Impro obtained were spoofed and accused Iran to be behind the attack [WB19]. Lloyd's list journal argues that it is likely that it was retaliation for the impounding of the Iran-controlled crude carrier Grace 1 [WB19].

However, according to C4ADS, a nonprofit organization that focuses on global conflict and security, only a small amount of all GNSS spoofing incidents are reported and publicly available [C4A19]. According to a report they released in 2019, 1311 civilian vessel navigation systems have been affected by GNSS spoofing events across

the Russian Federation, its occupied territories, and at locations where overseas military facilities are present between February 2016 and November 2018. Furthermore, the report identified the protection of Very Important Persons (VIPs), the protection of strategic facilities, and denial of airspace in combat zones to be the motivational factors that were the reason behind most of the incidents that occurred. As an example, GNSS spoofing has been assumed to be initiated to, among others, prevent unauthorized civilian drone activity in areas of interest to the Russian federation.

Several incidents affecting the navigational equipment to vessels where Nation states supposedly are behind have occurred. Both the spoofing incident in the black sea in 2017 and the spoofing incident in 2019 were close to waters controlled by the state allegedly executing the attack [WB19] [GPS17]. Additionally, the findings presented in the report to C4ADS identifies that the spoofing incidents took place at locations that are under the control of the Russian federation. It is as a result, likely that those types of attacks are conducted less frequently in areas where the most aggressive Nation states have limited jurisdiction and in international waters.

Hacktivists are driven by political or geopolitical decisions affecting national and international matters and is the fourth most active group. Website defacement and Distributed Denial of Service (DDoS) attacks are typical strategies to highlight their point and draw media attention.

Cyber Terrorists execute attacks that are typically harassing and disruptive. The group is driven by their political or ideological stand and execute attacks for financial gains, espionage, or to spread propaganda. ENISA describes cyber terrorists as a group with limited capabilities. However, the possible options related to attacks have increased as cybercrime-as-a-service has become more prevalent.

Script kiddies are the least active group and is a group which is assumed to have a limited set of capabilities. The group has no apparent motivation behind executing attacks and often utilizes tools and source code leakages that are available online. The lack of motivation makes the group somewhat unpredictable, which makes it hard to determine a threat level.

Chapter 3
Methodology

A research methodology allows readers to evaluate the reliability and validity of the research that has been completed. It is, therefore, important to choose methods that are suitable for the research project that is to be done. This chapter presents the four methods that were chosen to be used for the master thesis. Figure 3.1 shows an overview of how the methods have been used to answer the different research questions.

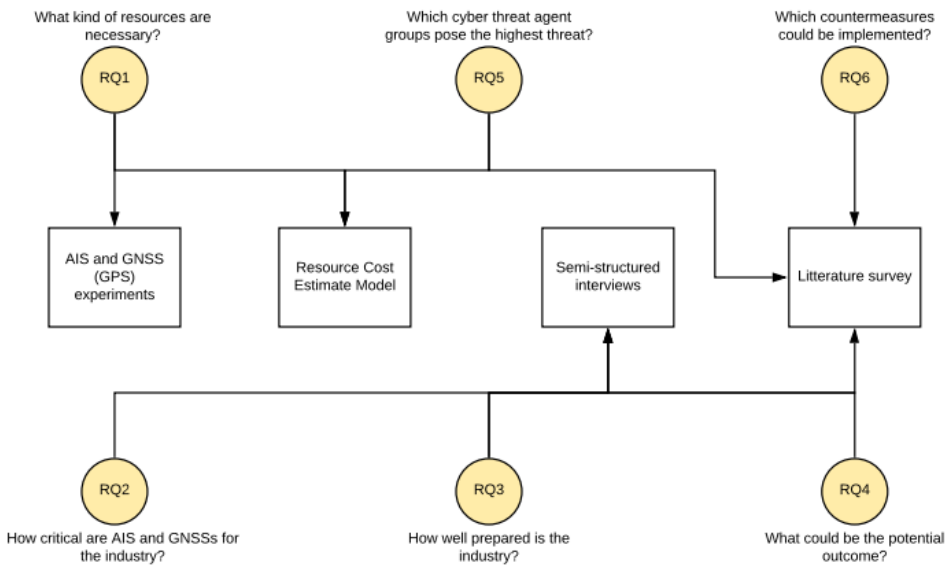


Figure 3.1: Mapping between research questions and methods

3.1 Literature study

The first step of the research conducted in this thesis consisted of a literature study. A literature study is a useful tool to get a better understanding of a topic by studying the research already done by others in the same problem area. The literature study helped shed light on which areas within the topic that needed further investigation. It was also used to formulate the questions that were used for the interview guide, which ensured that the interviews collected all the necessary information. When reviewing the literature, key points such as cybersecurity challenges, vulnerabilities, and proposed solutions were important topics.

A wide range of papers have been investigated by using academic search engines, such as Google Scholar, NTNU Oria, Science Direct, and dblp. These search engines serves quick and relevant research material without compromising on quality. The selected papers either directly or indirectly contribute to answer the research questions, or assist in understanding necessary background knowledge. The keywords that were searched for during the literature study included but are not limited to are; AIS, GNSS, maritime navigation systems, maritime cybersecurity, and vulnerabilities in navigation systems. Some of the relevant papers such as, *A security evaluation of AIS* [BPW14], are several years old, however, as explained in chapter 2, the problems described in the papers are still relevant today.

3.2 Experiments

The complexity of building, configuring, and executing attacks are often overshadowed by the results that are obtained by the attacks. As a consequence, the steps necessary to execute the attacks are oversimplified or even skipped, which often makes replications more exhausting than expected. To avoid assumptions regarding the complexity of performing AIS- and GNSS-based attacks, one experiment was done for each of the systems.

The GNSS-based (GPS-based) experiment was conducted in a lab environment on a mobile phone, as no equipment typically used to obtain GPS signals in the maritime industry were obtainable. Mobile phones use several technologies, such as GNSS, Wi-Fi, and cellular networks, to estimate the current position of the device. In order to manipulate the position by executing a GNSS-based attack, the connection to Wi-Fi and cellular networks needs to be switched off. However, this obstacle is not likely to be encountered with equipment used in the maritime industry, but was rather an obstacle encountered as a result of lack of optimal equipment. Furthermore, the vulnerabilities exploited in the experiment is something that affects all GPS receivers that are for non-military use. As disturbance of GPS signals can lead to disastrous outcomes on the devices affected and because it is illegal to transmit GPS

signals in an uncontrolled environment, a lab/room specifically made to contain electromagnetic signals was used.

The AIS experiment was conducted in a similar lab environment with similar limitations. No commercial AIS transceiver/receiver was obtainable. Instead, an SDR with open-source software was used to simulate a real AIS receiver. Thus, it is slightly harder to validate and ensure that the attacks executed will work in a real situation. It is also important to note that both experiments were done on devices located at a particular position and not moving. The static position that was set was due to the illegality regarding sending forged GPS and AIS messages, which required specialized rooms or equipment to prevent disturbance to real systems. The static position of the targeted devices results in coverage not being considered as an essential factor when executing the attacks. However, as discussed in chapter 6, knowing the coverage of attacks before executing is immensely important in a real scenario.

Moreover, AIS is an important system used for navigation and collision avoidance, and by disturbing the system, catastrophic outcomes could be possible. Consequently, several precautions were made to avoid interference with real systems. Firstly, the experiment took place several kilometers away from the nearest harbor. Secondly, the transmitting device transmitted with a low gain to reduce the range of the signal. Lastly, the experiment was conducted within a faraday cage, which is used to contain electromagnetic signals such as those sent by AIS transmitters.

The building, configuration, and execution of the attacks are described in great detail in chapter 4 and chapter 5.

3.3 Resource Cost Estimate Model

The model for estimating the cost of the required resources to carry out a cyberattack is based on the Intrusion Kill Chain and attack trees, which was an idea developed by Haga [Hag19].

Attack trees was developed by Schneier in 1999 [Sch99] and provide a formal way to evaluate the security of systems by utilizing a tree structure approach to present possible attacks. The tree structure is built up by a root node, which is the end goal of the attack and leaf nodes that are different ways to achieve the desired goal. The tree structure may also have intermediate nodes, which are sub-goals that are required to be fulfilled to achieve the root node goal. Furthermore, the tree typically consists of several branches, where each branch either is an ”OR” branch or an ”AND” branch. ”OR” branches have nodes that are independent of other nodes that have the same parent node and are hierarchically equivalent. These nodes are

commonly known as siblings, and siblings that are independent of each other only needs itself to be true to achieve the goal of the parent. ”AND” branches consist nodes that are dependent on all their siblings, and to achieve the goal of the parent, all the siblings have to be true. Figure 3.2 is an example of an attack tree, where each branch is considered an ”OR” branch unless stated otherwise.

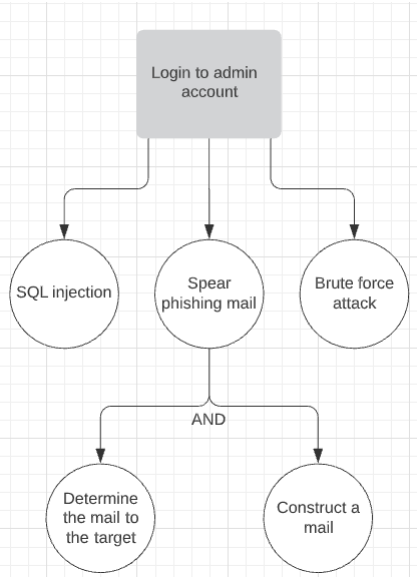


Figure 3.2: Attack tree example

The **Intrusion Kill Chain** was introduced by Hutchins et al. [HCA11] in 2011 and is a framework used to define the different stages in a cyber attack. By utilizing the framework, security analysts can identify and prevent potential intrusion attempts. It is important to note that traditionally, the model is used to detect and prevent Advanced Persistent Threats (APTs) targeting networks. The model is an Intelligence-Driven Computer Network Defense model, which consequently makes it important to understand the fundamental elements of intelligence known as indicators. The indicators are traces an adversary leaves behind and are used to detect the different stages in the kill chain ultimately. Hutchins et al. divided the types of indicators into three groups.

- **Atomic** indicators are the simplest form of indication that offensive activities are taking place. Examples of such indicators are emails and Internet Protocol (IP) addresses.
- **Computed** indicators are data that have been computed, such as hashes of malicious files.

– **Behavioral** indicators are a combination of indicators used to form a profile. Behavioral indicators can even use other behavioral indicators to form the profiles.

The model consists of seven typical stages a computer networked-based attack undergoes, from initial reconnaissance to completion.

1. **Reconnaissance**: The first stage in the chain is to research, identify, and select potential targets.
2. **Weaponization**: Secondly, an adversary couple an exploit with a deliverable payload, such as an email attachment.
3. **Delivery**: Thirdly, the adversary transmits the payload to the victim.
4. **Exploitation**: Fourthly, the adversary exploits a vulnerability to execute the malicious code.
5. **Installation**: Fifthly, the malware or the remote access is installed.
6. **Command and Control (C2)**: Sixthly, a C2 channel is established, which gives the adversary remote access to the victim's environment.
7. **Actions on Objective**: Lastly, after all the six previous steps are completed, the adversary can achieve its initial objective. An example of an objective can be the extraction of some specific data from the victim's environment.

Resource Cost Estimate Model

Haga used these two models as the base for the Resource Cost Estimate Model [Hag19]. The Resource Cost Estimate Model is a tool intended for cyber risk analysis and attacker profiling. This is done by identifying what kind of resources and costs that are necessary when executing cyber attacks. The Resource Cost Estimate Model combines each stage of Intrusion Kill Chain with an attack tree. For each stage of the Kill Chain model, an attack tree is constructed out of it, with the stage of Kill Chain as the root node. The trees constructed from each of the stages have all three levels. The root node is, as already stated, a specific stage of the Kill Chain. The root node is followed by an intermediate node that represents one or more resources, and lastly, one or more leaf nodes are present and represent resource alternatives. Leaf nodes are alternatives on how to obtain the resource in the parent node, and only one of them is needed to obtain resources from the parent. After all resources from the intermediate nodes are obtained, a stage in the Kill Chain may be completed. Figure 3.3 illustrates the structure of the model.

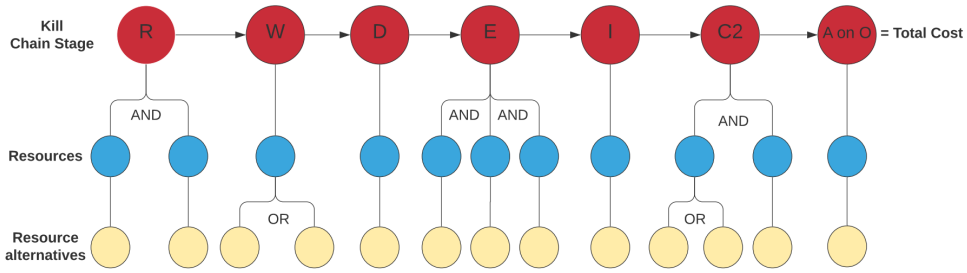


Figure 3.3: Resource Cost Estimate Model structure (inspired by [Hag19])

Cost Estimation

The model assumes that all seven stages of the Kill Chain are necessary to be completed to execute an attack successfully. Each stage has a cost associated with it, which is determined by what resources it is using. The cost of the resources is dependent on the resource alternatives that are available to achieve the resource. Resource alternatives have a minimum cost, a maximum cost, and a confidence associated with it, as shown in equation 3.1. The confidence ranges from 0 to 1 and indicates the likelihood of a correct cost interval. If the confidence is close to zero, several factors related to the cost are uncertain, which makes the cost interval likely to be incorrect. On the other hand, if it is close to 1, few factors are uncertain, and the cost interval is likely to be correct.

$$Estimated\,cost\ =\ [\,Min\,Cost,\ Max\,Cost,\ Confidence] \tag{3.1}$$

Before the total cost of the attack can be calculated, a set of resource alternatives able to achieve all the necessary resources need to be chosen. By default, the resource alternative with the lowest min cost or the highest max cost is chosen for each resource to obtain the total cost. This is, however, something that may be changed if a specific attack with specific resource alternatives are of interest. The total cost of the attack is then derived by taking the sum of all minimum cost estimates, and the sum of all maximum cost estimates of the chosen resource alternatives. Subsequently, the confidence of the cost interval is derived by taking the product of all the confidence to all the chosen resource alternatives. Equation 3.2, 3.3, and 3.4 formally describes how to calculate the costs and the confidence.

- $\mathbf{V}$ is a valid resource set for the attack.
- $\boldsymbol{\alpha}$ is the minimum cost of a chosen resource alternative.
- $\boldsymbol{\beta}$ is the maximum cost of a chosen resource alternative.

– **C** is the confidence of the chosen resource alternatives.

$$Min\,cost\ =\ \sum_{\substack{stage\,\epsilon\\ kill\,chain}}\ \sum_{i\,\epsilon\,V}\alpha_i \tag{3.2}$$

$$Max\,cost\ =\ \sum_{\substack{stage\,\epsilon\\ kill\,chain}}\ \sum_{i\,\epsilon\,V}\beta_i \tag{3.3}$$

$$Confidence\ =\ \prod_{\substack{stage\,\epsilon\\ kill\,chain}}\ \prod_{i\,\epsilon\,V}C_i \tag{3.4}$$

Resource Classes

The model classifies the following five types of resources:

Tangible resources are defined as physical items such as hardware components, antennas, and SDRs. Such resources typically have resource alternatives with a high degree of confidence, as these components, in most cases, can be bought commercially. However, this is not always the case as some items are illegal to sell, which makes a cost estimate harder to determine with a high degree of certainty compared to legal devices.

Logic-atomic resources are assets obtained by executing other cyber attacks not directly related to the undergoing attack. These assets might be passwords, IP addresses, or other types of information that are necessary for the goal at hand. Typically these assets can be acquired by exploiting human behavior by performing social engineering attacks.

Logic resources are resources such as software and data sets. As with tangible resources, some of the software might be commercially available, but this is not necessarily always the case.

Skill is related to the necessary effort an adversary needs to put in to develop potential needed software. The following equation determines the cost:

$$Price\ =\ l_c * n \tag{3.5}$$

l_c is the complexity related to write one line of code, and n is the number of lines written.

Behavioral resources are related to resources obtained by manipulating human behavior or by buying specific actions to be performed by a person. It is difficult to estimate a cost for this resource class because the chance that human errors occur or the cost associated with buying specific actions are extremely dependent on the person at hand. It is, therefore, hard to determine a cost interval of this resource with a high confidence.

The color mapping in figure 3.4 clearly distinguishes the different resource types.

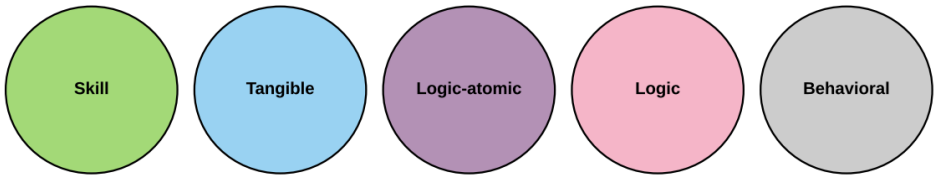


Figure 3.4: Colors used to identify different resources (inspired by [Hag19]

Why the Model is suited for the project

A part of this master thesis is to define what kind of resources that are necessary to initiate successful attacks on AIS- and GNSS-based systems. To be able to obtain a complete picture of the necessary cost, without neglecting important factors or steps, a kill chain may be used, as it identifies the necessary steps required to initiate an attack successfully. By combining the kill chain with attack trees, more granular information may be acquired. The Resource Cost Estimate Model also includes a broader range of resources, which makes it easier to separate costs between different entities and identifying the cost of a resource to a higher degree. The high level of granularity of the model makes it evident which steps of the attack are easily accessible, and which are not. The combination of the attributes explained in this sub-section are the main reasons for why the model suits well for this master thesis.

3.4 Semi-structured interviews

When investigating the current knowledge about cybersecurity in the maritime navigation systems, the empirical data for this thesis was collected through qualitative interviews, more specific, semi-structured interviews. Qualitative interviews are especially good at answering the ”how”, ”why”, and ”what” questions. This thesis uses a qualitative method rather than a quantitative method to gain in-depth information from selected interviewees. Interviews, as explained by Polit et al. [Pol10], is a method used to collect data by the use of verbal interchanges, where the goal is to obtain information from the interviewee.

Polit et al. differentiate between three different types of interviews: unstructured, semi-structured, and structured. Unstructured interviews are conducted without predetermined questions and resembles more a normal conversation. Structured interviews follow the same list of closed questions and can be beneficial when participants have either a speech or language impairment [Whi08]. However, they are often used to collect quantitative rather than qualitative data. Semi-structured interviews allows the interviewer to ask more open-ended questions, rather than a yes or no type of answer. The questions do not necessarily need to follow a predefined list of questions nor follow a specific order. This offers the interviewee the opportunity to reflect upon opinions, experience, and knowledge. It also allows the interviewer to see the topic from the interviewees perspective and understand why they have that perspective. The goal is to create a setting where the interviewer and the interviewee can discuss the topic in depth. The interview guide used for this thesis is accessible in Appendix A.

The flexible structure of semi-structured interviews allows the interviewer to go in-depth on topics where the interviewee has comprehensive knowledge. However, the interviewer is responsible for redirecting the interview if the conversation goes off-topic. According to Clifford et al. [CCGF16], a combination of different types of questions can be effective depending on the research topic. Questions can be crafted to elicit information that is thoughtful, emotional, descriptive, factual, or affectual. To create a relaxed conversation and pleasant atmosphere, the interviewer often start the interviews by asking questions that the interviewee feel comfortable answering. Difficult, sensitive, or questions that need considerable reflection is best left to the end of the interview when the interviewee is comfortable.

3.4.1 Participants

It is important to identify suitable interviewees to be able to gain valuable information from the interviews. According to Morse [Mor90], the interviewee must be knowledgeable about the topic, be able to reflect and provide detailed experiential information about the topic, and have the willingness to talk.

We interviewed eight participants from three various maritime stakeholders who use AIS and GNSS to assist them in daily tasks. The different stakeholders are explained more in detail in Chapter 7. With some help from our supervisor and a contact within the maritime shipping industry, we reached out to the stakeholders via mail to arrange interviews. The interviews were supposed to be conducted face-to-face to receive better and more comprehensive answers. However, due to the circumstances concerning COVID-19, only one interview was conducted face-to-face. The rest of the interviews were conducted by phone and Skype. As previously mentioned, the interview guide in Appendix A laid the foundation for the interviews. However, some questions were removed and added depending on the stakeholder interviewed. We found it interesting to interview participants from different stakeholders due to their different core activities. We assumed that this would result in better insight regarding how AIS and GNSS is used in different parts of the maritime industry.

3.5 Qualitative data analysis

The semi-structured interviews resulted in a significant amount of qualitative data. The raw data collected was unstructured text transcribed from the interviews. In order to sort, organize, and interpret the data, a method to analyze it was necessary. A Qualitative data analysis helps to transform the qualitative data into new knowledge, such as an understanding or explanation of the situation investigated. As explained by Thorne, there are several analytic strategies, such as constant comparative analysis, phenomenological approaches, ethnographic methods, narrative analysis, and discourse analysis [Tho00].

For this thesis, template analysis was the chosen method. The method is a part of a broad family of analysis methods, often referred to as thematic analysis, which depends on constant comparative analysis. These approaches identify similarities and differences in qualitative data so that it is possible to draw clear and explanatory conclusions associated with themes [GHC+13]. Template analysis is a great tool when the goal of the research is to find out something about people's experience, knowledge, and opinions from a collection of qualitative data such as interview transcripts. That is why the method was chosen for qualitative data analysis for this thesis. Template analysis includes the development of a coding template. This template summarises themes identified by the researcher as significant in a data set, and organizes them in a useful manner. The main procedural steps in performing template analysis are as following [BMTK15]:

- **Familiarization with data:**
  - The first step is to get familiar with the data to be analyzed. In smaller studies, for instance, ten or fewer hours with interviews, it would be

reasonable to listen or read through the data set at least once. In larger studies, the researcher might select a subset of the data, such as transcripts or field notes.

- **Preliminary coding:**
  - The second step is to carry out preliminary coding of the data. This process is typically the same in most thematic approaches, where the goal is to highlight anything in the data that contribute towards the researcher's understanding. However, template analysis often starts with some *a priori* themes, which are themes that are identified in advance and are expected to be relevant to the analysis. These codes are tentative and may be modified or removed if they do not contribute to the analysis.
- **Clustering:**
  - The third step involves sorting codes into themes, organizing them into meaningful clusters, and then defining how they relate to each other within and between the clusters. This process will include hierarchical relationships, where narrower themes is a part of broader themes. It may also include relationships between themes in different clusters at similar hierarchical levels. Themes that are apart of several distinct clusters are often referred to as "integrative themes".
- **Producing an initial template:**
  - The goal of this step is to define an initial coding template. It is common to develop an initial version of the coding template based on a subset of the data that have been obtained rather than carrying out preliminary coding and clustering on the whole data set before defining the thematic structure. For example, in a larger study with Thirty face-to-face interviews, the researcher may carry out steps 1-3 on six of the interviews and create the initial template. Before creating an initial template from a subset of data, the researcher must be sure that the selected subset reflects the whole data set.
- **Applying and developing the template:**
  - After the initial template has been created, it is applied to further data. The researcher has to decide whether new data of potential relevance can be represented by the themes defined in the initial template. If the existing themes cannot represent the new data, the template might need adjustment. New themes may be added, and existing themes redefined. Rather than modifying the template after every time new data is analyzed, it is common to analyze a larger amount of data and then implement a

new version of the template if it is needed. The process of finding the right template is iterative and results in a comprehensive representation of the researcher's analysis of the data.

– **Final interpretation:**

  ◦ In the final step, the template is applied to the whole data set. Note that the template is never "finalized", new data might call for further adjustments in the template.

3.5.1 Our process

	Step	Our process
1.	Familiarization with data:	The interviews were conducted and notes were written along the way and in hindsight.
2.	Preliminary coding:	Relevant data were coded using NVivo. The research questions formed the basis for a priori codes.
3.	Clustering:	The codes were grouped and produced three distinct themes.
4.	Producing an initial template:	The initial coding template was created by the three themes.
5.	Applying and developing the template:	The themes were validated in relation to the whole data set to make sure that they covered it and to ensure that relevant data was not overlooked.
6.	Final interpretation:	Merged with step 5

Starting at step 1, we got familiar with the data by taking notes both during the interviews and afterward, before analyzing it at a later stage. Since we did all the work with the interviews our self, we continuously worked with the data during collection and processing. During the second step, our research questions were used as a priori codes. Further, the qualitative data analysis software NVivo[1] was utilized for reviewing and structuring the notes, highlighting interesting information, and coding it in relation to the research questions. Some data was not represented by the a priori codes and was therefore marked as irrelevant for the thesis. After coding the data obtained by the interviews, the analysis moved into the next step. In step 3, our a priori codes derived from the research questions produced three themes: AIS and GNSS dependency, Awareness and preparedness, Potential outcomes of attacks. These three themes created the initial coding template in step 4. Since we only

[1] https://innsida.ntnu.no/wiki/-/wiki/English/NVivo

conducted eight interviews, we created the initial coding template from the whole data set instead of a subset. After creating the template, we moved on to step 5, the goal of this step is, as previously mentioned, to apply the coding template to further data. Since the template was created from the whole data set, we had no further data to apply to the template. Instead, we validated the themes in relation to the whole data set. The whole data set was once again analyzed to make sure that the themes represented it and to ensure that relevant data was not overlooked. The final step merged into step 5 since we already had applied the template to the entire data set.

The process resulted in a coding template consisting of three clearly defined themes. The themes and their definitions are as following:

- **AIS and GNSS dependency:** How critical are AIS and GNSS when sailing and does it exist any backup systems if they fail.
- **Awareness and preparedness:** How aware are people who engage with AIS and GNSS daily of the vulnerabilities in the systems. Are they prepared if someone was to exploit these vulnerabilities?
- **Potential outcomes of attacks:** Worst case scenarios if a successful AIS and/or GNSS attack occurs.

Chapter 4
GNSS (GPS) Experiment

4.1 Introduction to the experiment

This chapter demonstrates how to conduct two different types of spoofing attacks. First, a static spoofing attack will be conducted. The attack transmits signals causing the receiver to estimate an incorrect position. The second attack is trajectory-based, and unlike the static spoofing attacks, a trajectory-based attack specifies a direction and the speed at which the position changes.

One of the first challenges an adversary needs to overcome when trying to initiate either a static or a trajectory-based GNSS attack, is forcing the victim's receiver to lock onto the false signal. According to Psiaki et al., there are two ways to overcome this challenge [PH16a]. By disrupting the tracking of legitimate signals, which can be conducted by utilizing a jammer and then induce re-acquisition. Alternatively, by forging a signal that is code-phase and Doppler-matched with the legitimate signal. The latter is considerably harder to perform, especially in this particular experimental environment. There was no need for a jammer as the lab itself acted as a jammer since it was blocking out legitimate signals. However, this is something that needs to be considered when an attack is to be executed.

This experiment initiated the spoofing attacks only based on re-acquisition, however it was conducted without the use of a jammer.

It is important to note that GPS operates within the following three frequency bands; GPS L1 band (1575.42MHz), GPS L2 band (1227.6MHz), and GPS L5 band (1176.45MHz) [GOVa]. Currently, users can combine signals sent from the L1 band and the L2 to improve accuracy by using a dual-frequency receiver. However, the signals sent for public use at L2 and L5 are still deemed as pre-operational and should only be used at the user's own risk. Consequently, the experiment was only conducted over the L1 frequency band as it is the most established frequency band.

4.2 Experiment Setup

4.2.1 Overview

This section will describe the tools required to initiate both static and trajectory-based GPS spoofing attacks. Following is a detailed list of the hardware and software that was used to perform the attacks.

- Laptop computer, Ubuntu 18.04.3 LTS
  - Memory: 8 GiB
  - Processor: Intel® Core™ i3-6006U CPU @ 2.00GHZ x 4
  - Graphics: Intel HD Graphics 520 (Skylake GT2)
  - OS type: 64-bit
- Software components: GNU Radio, GPS-SDR-SIM, UHD
- SDR: Universal Software Radio Peripheral (USRP) B200mini, 70MHz - 6 GHz frequency range, full-duplex, USB 3.0 connectivity
- Receiver of signals: Motorola g6 plus, Android version 9

4.2.2 USRP B200mini

The Universal Software Radio Peripheral (USRP) B200mini is a software-defined radio/cognitive radio manufactured by Ettus research and covers a wide frequency range (70Mhz - 6GHz) [Resa]. This wide frequency range makes it possible to operate the radio on the frequency (GPS L1) where GPS signals for public use are transmitted. The device is also compatible with the GPS-SDR-SIM, which is a software component that assists the radio transmitting the data in a correct format. The device also has a USB 3.0 connectivity, which makes it easy to operate wherever a battery pack with a USB connection is available. In addition to this, the device is quite small, as shown in figure 4.1, and is as a result, physically hard to detect.

The USRP B200mini is mounted with two antennas of the type W1900, which are produced by Pulse Larsen. The antennas are most effective on the following frequency bands; 850MHz, 900MHz, 1.8GHz, 1.9GHz, 2.1GHz [Pul]. As a consequence, the antennas are not intended for transmitting or receiving GPS signals. However, as no other alternatives were currently available, and due to the short transmission distance in this experiment, the problem was disregarded.

Figure 4.1: A USRP B200mini with a pen next to highlight the small size of the device

4.2.3 GNU Radio

GNU Radio is an open-source software project that works both as a standalone platform, and as a platform where additional Radio Frequency (RF) applications can be built on top [rad19b]. The software provides signal processing functions for implementing SDR applications and is based on the Python interpreted language. Also, functions written in C++ can be included in the Python project by using the open-source software tool Simplified Wrapper and Interface Generator (SWIG). SWIG generates an interface between Python and C++, which makes it seamless to create functions in GNU Radio with C++. As C++ is a more performance reliant language, time-sensitive functions are typically written in C++ rather than Python.

GNU Radio uses the flowgraph data structure through which data flows, to build applications [rad19a]. The flowgraph data structure consists of several nodes or blocks as they are called in the GNU Radio environment that are intertwined. The flowgraph is acyclic and consists of one or several source blocks, one or several sink blocks, and any amount of processing blocks between them. The source block is used as a mechanism to insert samples to flowgraph, whereas the sink is to terminate or export the processed samples from the flowgraph. Each of the blocks within the graph, ideally, does precisely one job and is as atomic as possible. In return, this helps the software to stay modular and flexible when more blocks becomes publicly available.

GNU Radio Companion (GRC) is a graphical tool which enables a simple way to connect blocks and build flowgraphs. The tool greatly decreases the complexity when building flowgraphs by letting the users get access to a Graphical User Interface (GUI), where the current state of the flowgraph can be observed. In addition, the tool offers a drag and drop functionality, which further simplifies the creating of flowgraphs. By utilizing this functionality, blocks with the desired properties can be inserted and connected by simply dropping it into the flowgraph and then dragging a line to where it should be connected. An example of how to create a flowgraph is visualized in figure 4.2. The figure shows how to generate a Fast Fourier Transform (FFT) plot of a fixed signal with a sample rate of 48kHz in GNU companion.

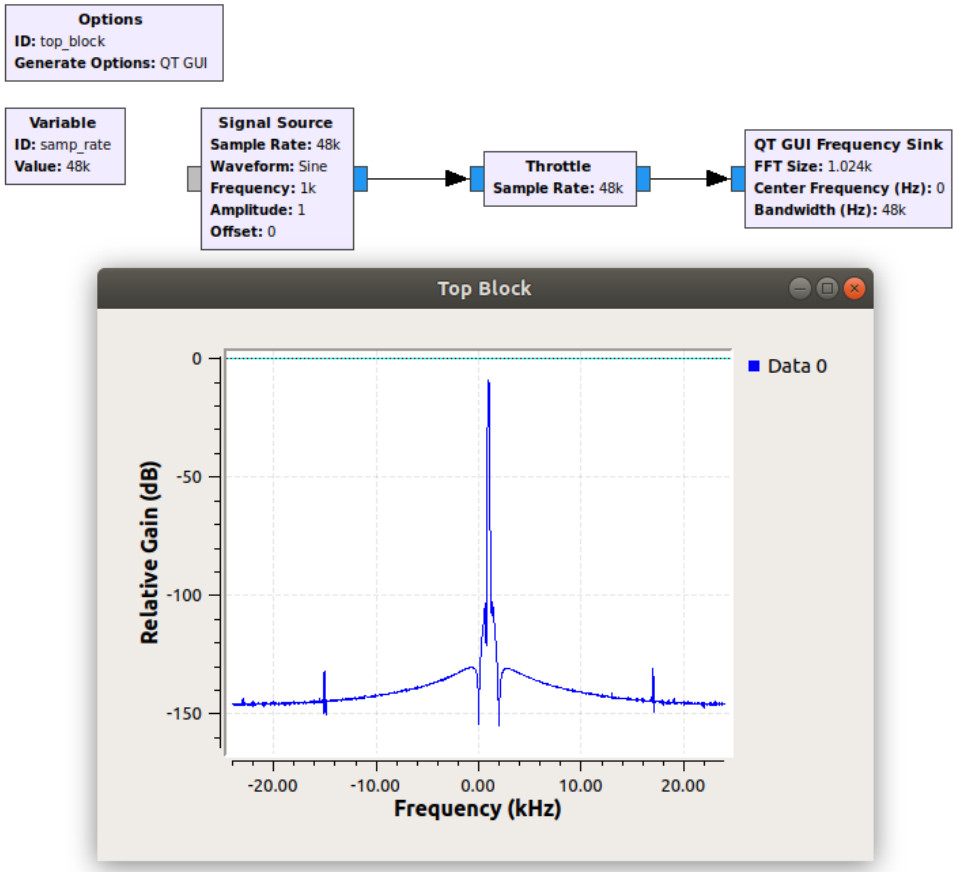


Figure 4.2: GNU Radio Companion: FFT of a fixed signal

4.2.4 GPS-SDR-SIM

GPS-SDR-SIM is a software that makes it possible to generate GPS baseband signal data streams, which then can be converted to radio frequencies by using SDRs [Ebi20]. The platforms that are known to be compatible with the software are; ADAML-Pluto, BladeRF, HackRF, and USRP. GPS-SDR-SIM can also generate both a user-defined trajectory and a static position as a GPS bin file, which opens up for a multitude of different possible attacks. The software is built on top of the GNU Radio software and is compatible with the latest version (3.8.x).

4.2.5 UHD

The USRP Hardware Driver (UHD) is a necessary prerequisite to communicate with a host computer when using USRPs [Res20]. The UHD provides the required tools to transport waveform samples to and from USRP hardware, and also allows users to control several parameters such as sampling rate and gains. The driver can be easily installed by the following guide created by Ettus [Res13], and the command **$ uhd_find_devices** can be executed to verify a successful installation.

4.3 Experiment: GPS Spoofing

The following GPS spoofing experiment was conducted inside a lab (C-451) located at the Electrical Engineering building at NTNU in Trondheim. A Faraday cage within the lab was used, which blocks electromagnetic waves such as radio waves. By using a Faraday cage, no other devices outside the experiment was disturbed by the signals transmitted. As a last precaution, an analysis of the frequency spectrum was conducted outside of the Faraday cage to ensure that no signals leaked out, which could cause disturbance to other devices.

4.3.1 Overview

The goal of the experiment was to evaluate the simplicity, cost, and equipment needed to launch a simple static GPS spoof attack, then looking at more advanced alternatives. The experiment was launched using a USRP B200mini to transmit GPS signals, and a Motorola g6 plus with android version 9 as the victim to be spoofed.

4.3.2 Procedure, Static GPS spoof attack

To be able to spoof GPS signals, the spoofer has to obtain precise information regarding the orbit to the GPS satellites. This information, which is known as ephemeris, is free and available on an anonymous File Transfer Protocol (FTP) service hosted by NASA. This service will, however, be discontinued on October 31, 2020 [NAS20]. Despite this, an alternative service that is not anonymous will be

available after this date. The anonymous service which gives access to ephemeris data is available at: **ftp://cddis.gsfc.nasa.gov/gnss/data/daily/**

The files obtainable from the service makes it possible to generate simulated pseudorange and Doppler for real GPS satellites. By using the generated data, digitized samples for the GPS signals can be created. The samples are stored in different ways, depending on the type of SDR is in use. In the case of USRP B200mini, the samples were stored as signed 16-bit integers. The required sampling rate also varies depending on the SDR. The USRP B200mini required a sampling rate of 2.5Mhz. Both of the requirements had to be accounted for when creating the samples.

After building the gps-sdr-sim software, the necessary command to create a sample file for the USRP follows:

Listing 4.1: Generation of sample file

```
#!/bin/bash
./gps-sdr-sim -e <broadcast ephemeris file (brdc)>
-b 16  -s 2500000 -l <latitude, longitude, height>
```

The command in Listing 4.1 results in a binary file, which can be transmitted by the USRP by executing the following command:

By executing the command in Listing 4.2, the USRP starts transmitting the forged GPS signals. However, in this experiment, the command did not result in a successful spoofing attack as it typically should.

Listing 4.2: Transmission of forged data

```
#!/bin/bash
 ./gps-sdr-sim-uhd.py -t gpssim.bin
 -s 2500000 -x <gain dB>
```

A possible reason why the attack using the python script (gps-sdr-sim-uhd.py) was not successful, could be related to the clock rate obtained by the USRP when the script was executed. The script did not enable the user to specify the clock rate, and thus forced the USRP to use a clock rate of 40.000000 Mhz.

The issue with the python script (gps-sdr-sim-uhd.py) was, however, a known issue created in 2016, affecting the USRP B200mini. The issue was closed in 2016, and the conclusion was that there were some problems in the gps-sdr-sim-uhd python file [And16]. Despite this being a known problem, the guidelines on how to correctly spoof GPS signals by using UHD devices have not yet been updated.

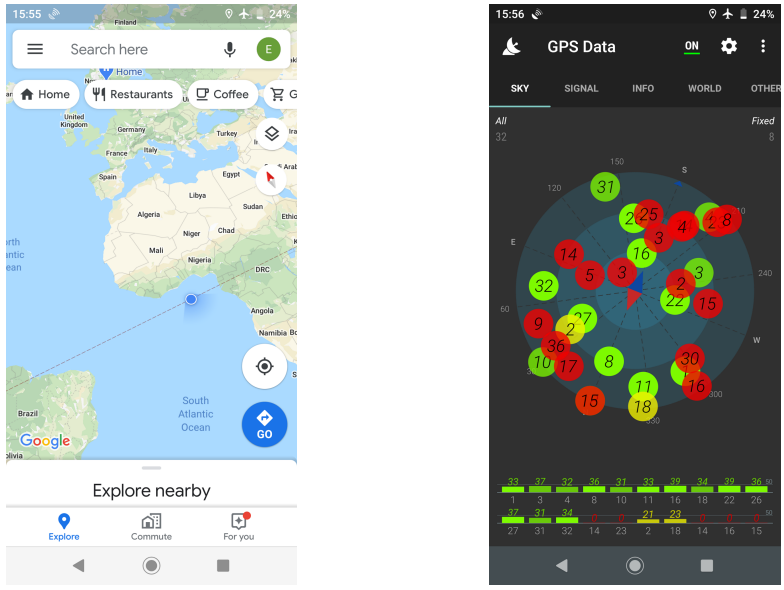
The solution to the problem was, however, to download an example file named tx_sample_from_file, from Ettus Research's UHD repository [Res19]. This c++ script made it possible to specify the clock rate (50.000000 Mhz) when sending a binary file and resolved, therefore, the current problem.

The command in Listing 4.3 was used to spoof the cell phones location successfully.

Listing 4.3: Transmission of forged data

```
#!/bin/bash
./tx_samples_from_file --args="master_clock_rate=50e6"
--file gpssim.bin --type short --rate 2500000
--freq 1575420000 --gain 0 --repeat
```

Figure 4.3a shows the spoofed location when opening google maps at the victim's phone. The location depicted in the figure has a latitude and longitude equal to 0 and height equal to 100. Figure 4.3b illustrates the different attributes of the signals transmitted by the USRP using the android application "GPS data". The application shows attributes such as the signal strength from the different spoofed satellites and whether the device has fix/locked itself onto a satellite or not. As the number of fix is over 4, it is possible to determine a precise location.



(a) Google maps showing spoofed location **(b)** GPS Data showing signal strength and fix

Figure 4.3: Google maps and GPS Data while being under a spoofing attack

4.3.3 Procedure, Trajectory-based GPS Spoof Attack

Trajectory-based GPS spoofing attacks typically tries to simulate the movement of the victim, as a way to fool the victim to believe the received GPS data is legitimate. This type of attack is often harder to detect compared to the static spoof attack and a jamming attack because the received GPS data seems legitimate, and the service is seemingly as usual.

The gps-sdr-sim enables trajectory-based GPS spoof attacks, but requires that the spoofed trajectory is specified either in a CSV file with Earth-centered Earth-fixed (ECEF) user positions or as an NMEA GGA stream. ECEF specifies user positions as x,y, and z coordinates where the point (0,0,0) is the center of mass of the earth. An NMEA GGA stream also contains information such as position but has additional information such as the number of satellites used.

In the case of an NMEA GGA stream, to generate it, the free software SatGen was used [Lab]. By feeding SatGen a KML file, an NMEA GGA stream can be created. The KML file contains the spoofed path in Google Earth, as shown in figure 4.4. By downloading the KML file and importing it to SatGen, an NMEA file can be created. Several dynamic settings can also be adjusted in the SatGen software to optimize the attack.

To be able to initiate the attacks, the digitized GPS signals need to be created by using the command in Listing 4.4

Listing 4.4: Generation of sample file for a trajectory-based attack

```
#!/bin/bash
./gps-sdr-sim -e <broadcast ephemeris file (brdc)> -b 16
-s 2500000 -g <NMEA file>
```

Lastly, the attack is executed by performing the command in Listing 4.5

Listing 4.5: Transmission of forged data

```
#!/bin/bash
./tx_samples_from_file --args="master_clock_rate=50e6"
--file gpssim.bin --type short --rate 2500000
--freq 1575420000 --gain 0 --repeat
```

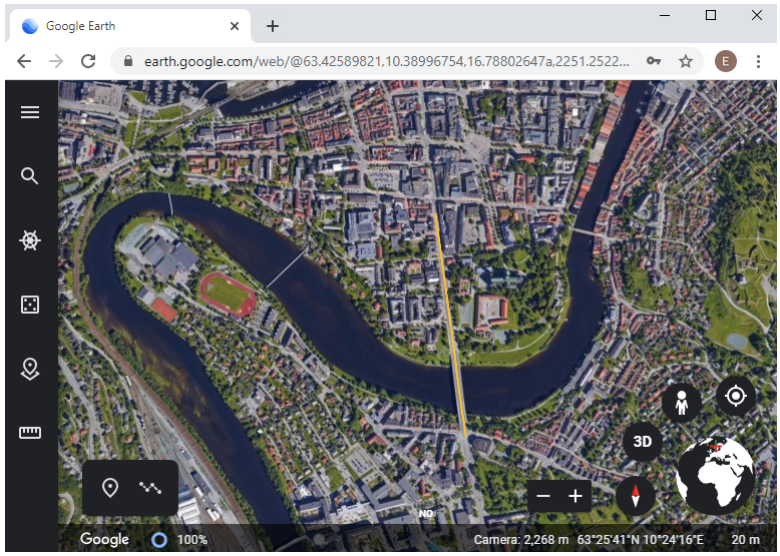


Figure 4.4: Google Earth trajectory that was spoofed (orange line)

4.3.4 Alternative platforms

The gps-sdr-sim software supports several platforms, and the experiment was reproduced with the HackRF. By following the guidelines available on the gps-sdr-sim GitHub repository [Ebi20], GPS signals were seemingly produced. No obstacles were encountered before this point, however after the transmission started, the receiver was not able to obtain a fix and indicated that something was not properly working. Takuji Ebinuma, a developer of the software, argues that the crystal of the HackRF may not be precise enough, as the crystal in the HackRF is a simple crystal without any temperature compensation [Meh15]. This could lead to a frequency offset that is larger than the frequency search range of the receiving device. Nevertheless, the issue can be fixed by buying a Temperature-Compensated Crystal Oscillator (TCXO) module and then mount it on the HackRF circuit board. However, this was never tested, as a physical modification of the HackRF was necessary.

Chapter 5
AIS Experiment

5.1 Introduction to the experiment

This chapter will explain the tools and steps necessary to set up and launch several AIS-based attacks. The experiment was completed in a closed environment with two SDRs. One SDR was acting as a receiver while the other SDR was acting as the transmitter. The reason behind using an SDR as the receiver rather than a commercial AIS receiver/transceiver, which would be preferable, was due to not having access to a commercial AIS receiver/transceiver. The lack of AIS equipment should, however, not affect the results as the SDR receiver can receive, decode, and react to the generated AIS messages in a similar way to the commercial AIS receiver/transceiver.

The experiment only conducts a subset of known attacks that are possible when forging fake AIS messages. AIS supports a wide range of messages, and as a way to keep the experiment concise and interesting, only the most severe attacks are covered.

5.2 Experiment Setup

5.2.1 Overview

This section will give an overview of the necessary tools required to perform different types of AIS related attacks. Following is a detailed list of the hardware and software used to perform the attacks.

- Computer, Ubuntu 18.04.4 LTS
  - Memory: 32 GiB
  - Processor: Intel® Core™ i7-4790 CPU @ 3.60GHz × 8
  - Graphics: Intel® Haswell Desktop
  - OS type: 64-bit
- The experiment ran within two Virtual Machines (VMs)
  - Receiver VM
    - Memory: 10 GiB
    - Processor: Intel® Core™ i7-4790 CPU @ 3.60GHz × 3
    - llvmpipe (LLVM 9.0, 256 bits)
    - OS type: 64-bit
  - Transmitter VM
    - Memory: 10 GiB
    - Processor: Intel® Core™ i7-4790 CPU @ 3.60GHz × 3
    - llvmpipe (LLVM 9.0, 256 bits)
    - OS type: 64-bit
- SDR: Two USRP B200minis, 70 MHz - 6 GHz frequency range, full-duplex, USB 3.0 connectivity
- SDR: One HackRF One, 1 MHz to 6 GHz frequency range, half-duplex transceiver, supported sample rates from 2 Msps to 20 Msps (quadrature), USB connectivity
- Transmitter, Software components: AISTX, GNU radio, gr-osmosdr
- Receiver, Software components: gr-ais, Socat, OpenCPN, and UHD

5.2.2 HackRF One

HackRF One is an SDR peripheral manufactured by the Great Scott Gadgets. The SDR has a frequency range from 1 MHz to 6 GHz, which makes it capable of operating at the frequencies where AIS messages are transmitted [Oss17]. HackRF is as the USRP, powered by USB, which makes it simple to operate at a multitude of desired locations. It is an open-source platform and can be used either for stand-alone operations or as a USB peripheral. Throughout this experiment, the HackRF will be used as a USB peripheral, as stand-alone operations will not be necessary.

The HackRF is mounted with one antenna manufactured by Delock with item number 88451 [Del]. The antenna is developed to operate the frequencies on the GSM, the UMTS, and the LTE bands and has a frequency range of 900 - 960 MHz, 1710 - 2170 MHz, and 2570 - 2620 MHz. Despite not being optimized for the frequencies where AIS operates (161.975Mhz and 162.025Mhz), it was considered sufficient as the signals in the experiment were transmitted over a short distance.

Figure 5.1: HackRF One with a pen next to highlight the size of the device

5.2.3 AISTX

AISTX is built on top of GNU radio and was developed by Balduzzi et al. [BPW14]. The software enables communication over both of the channels where AIS messages are transmitted (161.975MHz and 162.025MHz). Transmission is also independent of each other, which makes it possible to transmit different messages simultaneously on both channels. This functionality is a necessity under some attacks on AIS.

As mentioned in section 2.2, AIS transmitters have a total of 27 specific message types, each of which has an individual purpose. The messages or sentences, as they traditionally are called, are defined in the AVIDM protocol, which is the application layer protocol AIS uses when transmitting messages. Balduzzi et al. have developed an encoding tool in Python as part of the AISTX software, which makes it possible to specify the message type to transmit [BPW14]. This encoding tool enables a variety of attacks in addition to the more typical spoofing and DoS attacks.

However, the software suffers from a lack of maintenance. Balduzzi states that the researcher group is not allocating time to maintain the code, as the research is completed [Mic17]. Consequently, building the software becomes more time consuming as packages become incompatible with the software due to updates and require that the packages are downgraded.

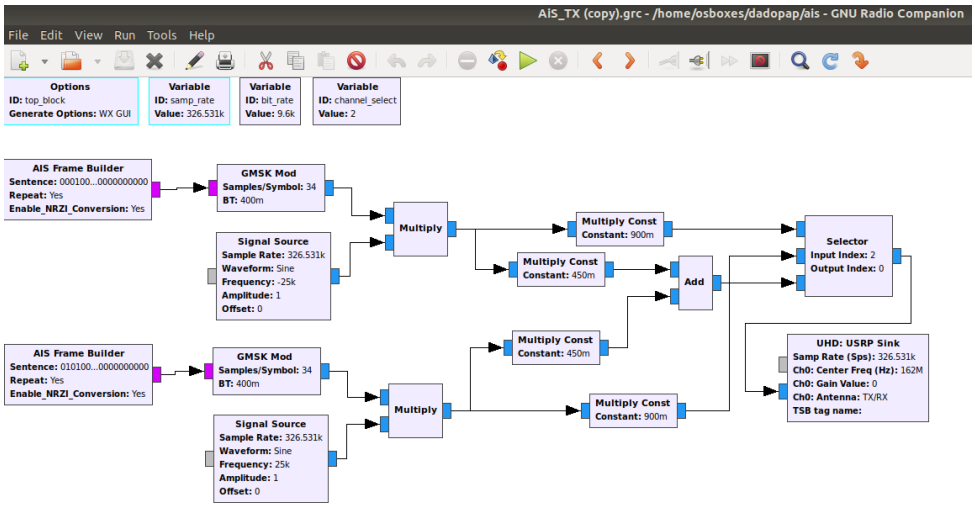


Figure 5.2: Flowgraph AISTX

5.2.4 gr-osmosdr

The gr-osmosdr software contains GNU radio blocks for interfacing with a variety of radio hardware, which is not supported by GNU radio by default [go]. The software is primarily developed for OsmoSDR hardware, but also support other hardware devices such as the HackRF.

5.2.5 gr-ais

gr-ais is an open-source AIS receiver software built on top of GNU Radio [Fos]. In this experiment, the software is used by the USRP to detect and decode messages sent on the dedicated AIS frequencies. The messages can then be interpreted by a visualization software such as OpenCPN.

5.2.6 Socat

Socat is a command-line-based utility tool used to create bidirectional data streams [Deb]. The streams can be constructed from a wide range of data sinks and sources. When establishing a data stream, the address command line arguments need to be constructed, which will give Socat necessary instructions to establish the stream. An address consists of three components, the address type, address parameters, and address options. In the case of this experiment, the address type is the pipe with a filename required as the address parameter. The complete address follows this form, pipe:<filename>.

5.2.7 OpenCPN

OpenCPN is a free software project which implements a fully functional chart plotter [Ope]. The software supports all types of AIS messages, and makes it simple to visualize moving vessels. The software will be used in the experiment to render the result of the attacks visually. The software offers a wide range of maps that can be used as an overlay to get more detailed information about the surroundings. However, in the case of the experiment, no such map was used as it was deemed unnecessary.

5.3 Experiment: AIS spoofing

The experiment setup consists of two SDRs, one that acts as a transmitter and one that acts as a receiver. Originally two USRPs were the intended equipment, as the required software seemed to be compatible with the USRP. However, after being unable to transmit messages with the USRP, the HackRF One was chosen instead. Section 5.3.1 will point out the obstacles encountered, which were the reason behind this change.

5.3.1 Configuration and building the software

Due to a lack of documentation and maintenance of the software, more obstacles were encountered when building it compared to the software used in chapter 4. The building of the software and the prerequisite requirements will, therefore, be explained in greater detail compared to section 4.3.

Configuration and Building (Receiver side)

gr-ais is compatible with the GNU radio 3.7 version (legacy) and was the version used throughout this experiment. The building and installation process of the gr-ais, OpenCPN, Socat, and GNU radio was a straight forward process without complications. Following are the commands that were executed to set up the software:

Listing 5.1: GNU radio 3.7.x: Dependencies

```
#!/bin/bash
sudo apt install cmake git g++ libboost-all-dev \
python-dev python-mako python-numpy python-wxgtk3.0 \
python-sphinx python-cheetah swig libzmq3-dev \
libfftw3-dev libgsl-dev libcppunit-dev doxygen \
libcomedi-dev libqt4-opengl-dev python-qt4 libqwt-dev \
libsdl1.2-dev libusb-1.0-0-dev python-gtk2 python-lxml \
pkg-config python-sip-dev graphviz
```

Doxygen dot was a needed component, but was not a part of the required packages on the wiki page to gnuradio [Gnu20]. The component was added by installing the graphviz package.

Listing 5.2: GNU radio 3.7.x: PPA installation

```
#!/bin/bash
sudo add-apt-repository ppa:gnuradio/gnuradio-releases-3.7
sudo apt-get update
sudo apt install gnuradio
```

Listing 5.3: gr-ais: Installation

```
#!/bin/bash
git clone https://github.com/bistromath/gr-ais.git
cd gr-ais
mkdir build mkdir && cd build && cmake ../ && make
sudo make install  &&  ldconfig
```

Listing 5.4: OpenCPN: PPA installation

```
#!/bin/bash
sudo apt-get install software-properties-common
sudo add-apt-repository ppa:openCPN/openCPN
sudo apt-get update
sudo apt-get install openCPN
```

Listing 5.5: Socat: Installation

```
#!/bin/bash
sudo apt-get install socat
```

Initialize the receiver: To set up the receiving end of the attack, a pipe where incoming data can be read from needs first to be established. By executing the command in Listing 5.6, a pipe is established.

Listing 5.6: Socat: Set up a pipe

```
#!/bin/bash
socat -d -d pipe:<name_of_pipe> pty&
```

In the terminal, Socat will reply with the name and the location of the created pipe.

2020/02/28 05:32:27 socat [2456] N PTY is /dev/pts/2

To be able to utilize the pipe in OpenCPN, a data connection needs to be added in OpenCPN. The data connection can simply be added within the options menu by specifying the data port, which in this case is /dev/pts/2.

Lastly, gr-ais is initiated, which starts the process where the USRP listens for AIS messages. The data is then recorded and then sent down the pipe, which makes

it possible for the OpenCPN to render the data visually.

Listing 5.7: USRP starts listening for messages

```
#!/bin/bash
ais_rx -suhd -g<specify_gain> -r250e3 > <name_of_pipe>
```

Configuration and Building (Transmitter side)

AISTX is compatible with GNU radio version 3.7. Therefore, executing the commands in Listing 5.2 can be used to build the GNU radio.

Listing 5.8: AISTX: Installation

```
#!/bin/bash
git clone https://github.com/trendmicro/ais.git
cd ais/gr-aistx
mkdir build && cd build

cmake .. -Wno-dev \
-DPYTHON_EXECUTABLE:FILEPATH=/usr/bin/python2.7 \
-DPYTHON_INCLUDE_DIR:PATH=/usr/include/python2.7 \
-DPYTHON_LIBRARY:FILEPATH= \
/usr/lib/x86_64-linux-gnu/libpython2.7.so

make
sudo make install
```

It was necessary to specify the used Python version as the Ubuntu environment kept using the 3.x Python version.

After building the software, two alternative scripts are available to execute the attack. The first option is to execute the attack using a Python script named AIS_TX.py. However, the script needed the following modification before it was executed, as one of the modules was not found at the current location.

Edit line 32: **from gnuradio.gr import firdes** with **from gnuradio.filter import firdes**

The second option is to execute the flowgraph located in the file AIS_TX.grc, which can be done through GNU companion.

Additional obstacles occurred when executing the program as the FPGA image

that was being loaded onto the USRP by the UHD driver was not compatible with the AISTX code, and the following error occurred:

Error RuntimeError: Expected FPGA compatibility number 5, but got 7

However, Ettus stores FPGA images before their update such that older versions can be acquired at their website [Resb]. Despite this, it was not trivial to determine the FPGA compatibility number before downloading it, and required several attempts before acquiring the correct image. The binary image with compatibility number 5 is located within the following zip file:

https://files.ettus.com/binaries/images/uhd-images_003.010.003.000-release.zip

By changing the FPGA image, it was possible to compile, build and transmit messages with the AISTX software. However, a new obstacle occurred, as the receiver was not able to obtain and decode the messages that were sent by the USRP. It became evident after eliminating possible factors on both the transmitter and receiver side, that the problem originated from the side of the transmitter. Several attempts, such as trying to modify the gain and sample rate, were tried to solve the problem without any success.

The solution to the problem was to modify the flowgraph of the software. The modification allowed the Hackrf to be used as the sink instead of the USRP. By default, AISTX only supports UHD devices acting as the sink. This was, however, manually modified by deleting the USRP sink shown in figure 5.2 and inserting the Osmocom sink, which is compatible with the HackRF hardware. The modified flowgraph is shown in figure 5.3. The Osmocom SDR block was not a part of the blocks that came with neither the GNU radio nor the AISTX installation. Therefore, the block was manually added by installing the gr-osmosdr software. The installation from the GitHub repository followed a standard CMake installation process as shown in Listing 5.9.

Listing 5.9: gr-osmosdr: Installation

```
#!/bin/bash
git clone git://git.osmocom.org/gr-osmosdr
cd gr-osmosdr/ && mkdir build
cd build && make
sudo make install && ldconfig
```

An alternative solution to the modification of the flowgraph would be to modify the AIS_TX.py script to make it compatible with the HackRF sink. These modifications were, however, not conducted.

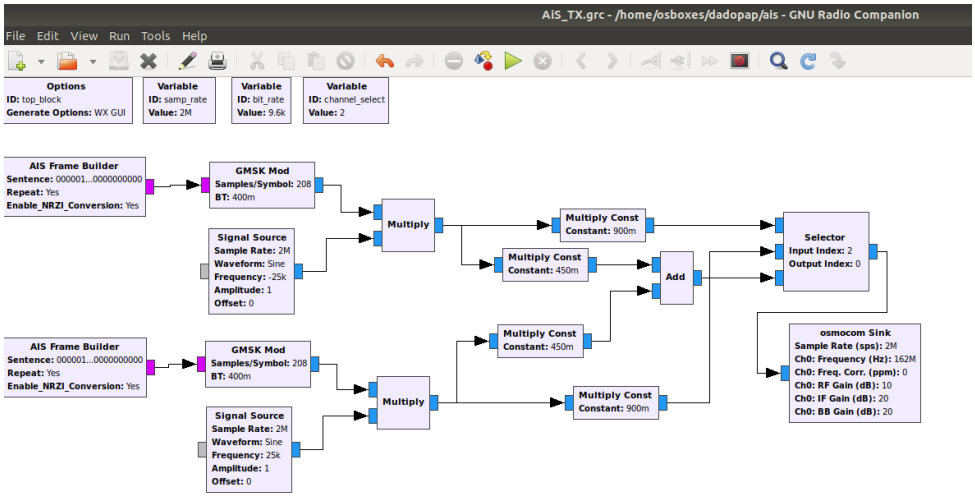


Figure 5.3: Modified AISTX flowgraph with osmocom sink

5.3.2 Procedure: AIS spoofing attacks

Trajectory-based vessel spoofing

As mentioned in section 2.2, collision avoidance is one of the essential features of AIS by utilizing a CPA alert. The feature is especially important when sailing in open waters where port authorities are not present and unavailable for navigational assistance. Trajectory-based spoofing attacks forge messages as a way to trick nearby victims into believing that a vessel is nearby and headed in a particular direction. A possible consequence of such an attack, is that it can cause a CPA alert to go off and force vessels to change their course to avoid collision with the spoofed vessel.

Several parameters need to be set and determined before initiating the attack. Firstly the type of message needs to be specified. As observed in Appendix B, Type 1 messages are reserved for messages containing positional information and, therefore, are suited for a trajectory-based vessel spoofing attack. Secondly, location, speed, and course of the vessel needs to be specified.

As with all the attacks carried out by AISTX, the first required step to initiate any attack is to encode the forged AIS message into an AIVDM payload. This is done by utilizing the AIVDM_encoder Python script, where the message to be encoded is specified.

Figure 5.4 displays a spoofed vessel and its trajectory outside the French island Corsica in OpenCPN. By specifying the desired parameters, encoding them as shown in Listing 5.10, and executing the command, a binary represented AIVDM

payload is returned. The AIVDM payload is then inserted into the sentence field of the AIS Frame Builder block/blocks (shown in figure 5.3 within the flow-graph and then executed. The upper AIS Frame Builder block is dedicated to messages sent over channel A (161.975 Mhz) while the lower AIS Frame Builder Block is dedicated to channel B (162.025 Mhz). It is important to note that both of the blocks do not need to have a valid sentence to be initiated successfully.

Listing 5.10: AIVDM encoding: Trajectory-based vessel spoofing

```
#!/bin/bash
./AIVDM_Encoder.py --type=1 --mmsi=247320170  --speed=75
--course=75 --long=9.344559 --lat=43.044153
```

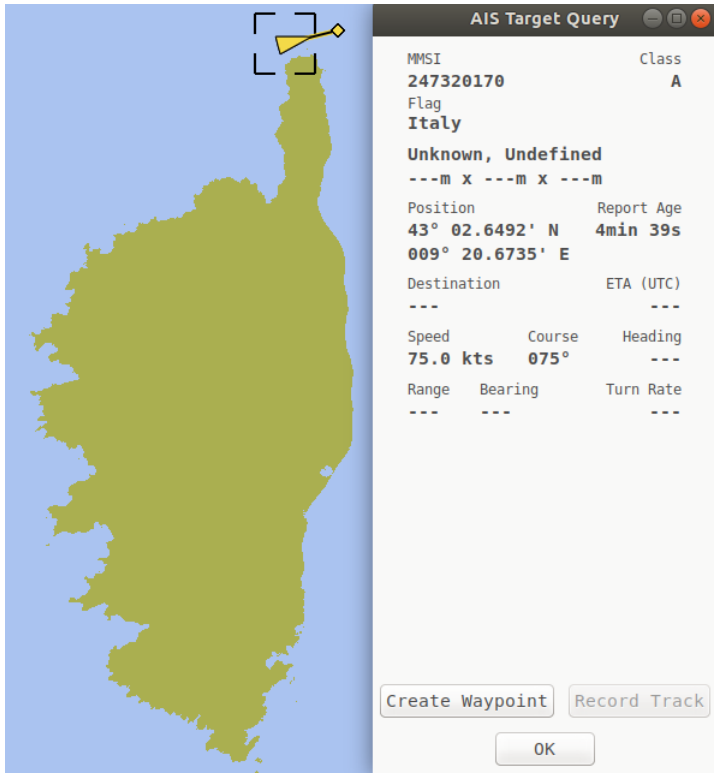


Figure 5.4: OpenCPN: Trajectory to a spoofed vessel outside the French island Corsica

AIS-SART Spoofing

Two types of devices are used in SAR operations, AIS-SART, or radar-SART. AIS-SART devices use AIS to transmit the position of a person overboard. As mentioned in section 2.2.2, vessels receiving this type of message is required by law to engage in a SAR operation. However, this message can be as easily forged as the spoofed vessel in the previous subsection. A SART message follows a standardized format where the Maritime Mobile Service Identity (MMSI) has the following structure, 970xxyyyy. The first three digits identify that messages are sent from a SART device. The 'xx' identifies the manufacturer where 00 is reserved for testing purposes, and lastly, the 'yyyy' is the sequence number set by the manufacturer. After specifying the MMSI following the standardized format, a location is the only necessary parameter needed before launching the attack. Listing 5.11 shows the command necessary to encode the forged AIS message into an AIVDM payload, and figure 5.5 shows the result of the attack.

Listing 5.11: AIVDM encoding: AIS SART spoofing

```
#!/bin/bash
./AIVDM_Encoder.py --type=1 --mmsi=970010000
--long=9.344559 --lat=43.044153
```

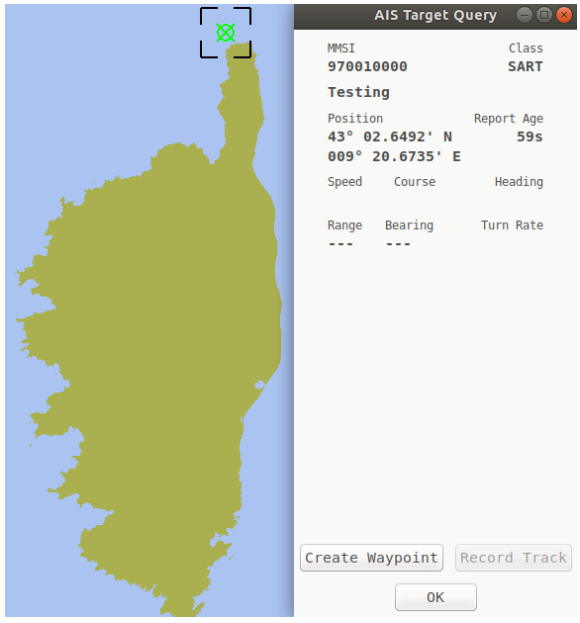


Figure 5.5: OpenCPN: Spoofed SART signal outside the French island Corsica

5.3.3 Procedure: AIS hijacking attack

AIS hijacking attacks are the second class of attacks possible with the AISTX software. This class of attacks exploits the opportunity to modify AIS messages without being easily detected. AIS hijacking attacks are explained in greater detail in the background Section 2.2.2. Section 2.2.2 also highlights two possible versions of the attacks, either as a man-in-the-middle attack in the software or by utilizing an RF component. The experiment conducted in this section is, however, focused on attacks that are possible by utilizing RF components. Despite this, the attack was not tested in practice throughout this experiment. This is a result of to be able to perform such an attack without disturbing real systems, two transmitters and one receiver are required. However, only one transmitter was obtained and made it, therefore, unfeasible to carry out an AIS hijack attack.

Theoretically, the RF-based attack starts by using the same IDs as the targeted victim, which makes it possible to masquerade as the victim. Then by emitting the AIS signals with a higher power than the victim, the message sent by the victim will be discarded, and the modified message sent by the attacker will be received and used instead.

5.3.4 Procedure: Availability disruption

Availability disruption attacks try to make AIS services unavailable for the victims. This class of attacks are divided into three sub-groups: slot starvation, frequency hopping, and timing attacks. The sub-groups are previously explained in section 2.2.2.

Timing attacks

Timing attacks use a VTS-reserved command to instruct AIS transceivers to delay their transmission of AIS messages. The attack uses the message Type 23, which is reserved for group assignment commands. Type 23 messages is intended to broadcast operational parameters used by all stations in the near vicinity. However, by specifying a desired target, the attack can be limited to only affect a specific victim, according to Balduzzi et al. [BPW14].

Listing 5.12: AIVDM encoding: Timing attack (1 minute)

```
#!/bin/bash
./AIVDM_Encoder.py --type=23 --quiet=1
```

In this experiment, it is difficult to verify whether such an attack is successful or not, as the setup does not consist of a commercial AIS transceiver that regularly transmit AIS messages. Nevertheless, in OpenCPN, the forged messages are accepted by the

receiver, as shown in figure 5.6, and indicates that the attack was successful. It is also important to note that no alert was given when the message was accepted, which makes it hard to detect such an attack when successfully conducted. The attack can also be repeated several times to increase the transceivers transmission delay. In addition, the transmission delay can be adjusted to a desired value.

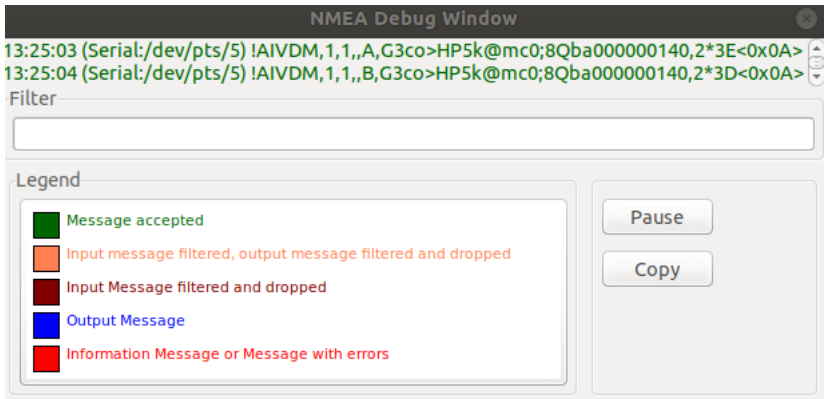


Figure 5.6: NMEA Debug Window: Accepted Timing attack messages

Frequency Hopping

Frequency hopping attack uses Type 22 messages reserved for a control authority to force AIS transceivers to change the frequencies they are currently operating on. Type 22 messages are initially intended for channel management purposes. AIS messages usually are transmitted and received over channel_a=2087 and channel_b=2088, but by modifying these fields, an AIS transceiver will be forced to change their frequencies for channel a and b. As a consequence, the AIS transceiver will not be able to receive nor transmit messages. Listing 5.13 shows the necessary parameters to perform frequency hopping. This attack can also be limited to a specific area by setting the sw_lat, sw_long, ne_lat, and ne_long fields.

Listing 5.13: AIVDM encoding: Frequency Hopping

```
#!/bin/bash
./AIVDM_Encoder.py --type=22 --channel_a=2080
--channel_b=2081
```

In the case of this attack, the AIS receiver accepted the forged AIS messages, as shown in figure 5.7. In a similar fashion as the timing attack, no notification was given when the AIS messages were accepted, which would make this attack hard to detect when executed. Despite accepting the messages, the receiver did

not change frequencies, and it was still able to receive messages at the standard channels after the attack was executed. The reason why the receiver did not change its frequencies is however unclear. For future work, the attack should be carried out using a commercial AIS transceiver. This will verify whether the issues are related to the setup of this experiment, or whether the attack was executed incorrectly.

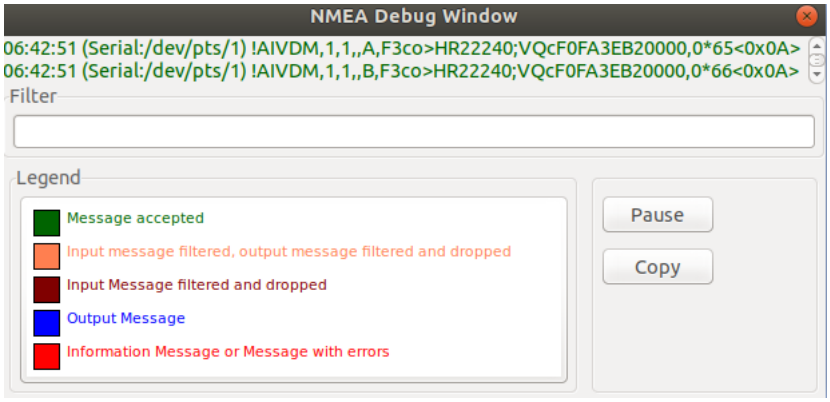


Figure 5.7: NMEA Debug Window: Accepted Frequency Hopping messages

Slot Starvation

The Slot Starvation attack is a similar Denial of Service (DoS) attack as the Timing attack and the Frequency Hopping attack. As this attack also is hard to verify without commercial AIS equipment, it was never conducted in this experiment. Theoretically, the attack uses the Type 20 message, which is a Data Link Management Message, to pre-allocate TDMA slots, which results in no available slots for users in the near vicinity. Consequently, no AIS transceivers close to the attack will be able to receive and transmit messages.

Chapter 6
Resource Cost Estimate

AIS- and GNSS-based attacks have been known to be possible for quite some time. However, most research within the field have focused on the potential outcome or potential mechanisms that may thwart such attacks and not on identifying potential threat agent groups and the resources needed to carry out such attacks.

This chapter will explore resources necessary to carry out the attacks initiated in chapter 4 and 5 on vessels in the maritime sector by using the Resource Cost Estimate Model defined in section 3.3.

6.1 Cost Estimation

The following section will present an in-depth review of the resources necessary to carry out the attacks discussed in chapter 4 and chapter 5 on operational systems and estimate an associated cost. For this cost estimation, the attacks target large vessels required to have operational AIS and GNSS equipment onboard. Some identified resource alternatives in the following models have not been associated with a cost. This is because some estimates would be largely based on personal opinions and consequently do not contribute to estimate the cost. Additionally, a golden line is placed around the resource alternatives that have been chosen as the base for the cost estimate. The choices are determined based on what is considered to be the most likely alternatives, which at the same time has an associated cost that is assumed to be close to reality.

6.1.1 GNSS spoofing (re-acquisition)

Reconnaissance

During the reconnaissance stage, it is important to determine the vulnerability to exploit, who to target, and how to deliver the malicious payload. In the case of GNSS spoofing attacks, two branches have been created, as shown in Figure 6.2.

Firstly, the position and the route of the target needs to be obtained to ensure that it is possible to intercept the targeted vessel at some part of the route. Three resource alternatives were identified as potential methods to determine the route and position. The method considered as most likely is through an AIS-based application. Marine Traffic offers such an application, both for free and for 190.80 $ per month [Mar]. The free version is, however, somewhat limited as it does not offer a global view, and only minimal information is offered regarding the route. Nevertheless, the free version still offers valuable information, as shown in Figure 6.1. The premium version offers more information and enables access to the most recent positions received by satellite, a global view, and enhanced information regarding the route.

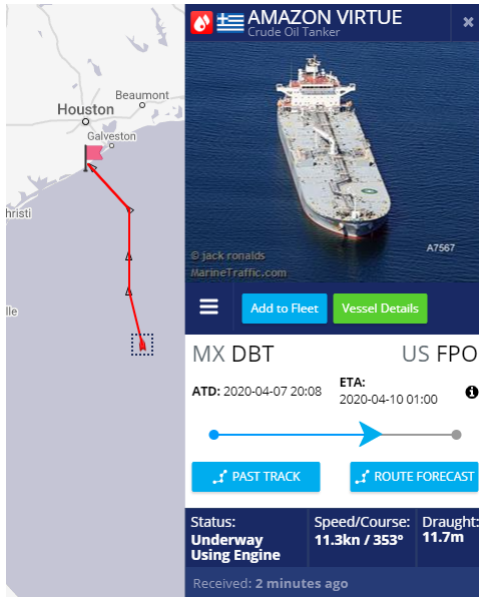


Figure 6.1: Marine Traffic: Free service

Secondly, to estimate the coverage of the attack, three alternatives were discovered. Optimally, a practical experiment should take place, as it is the method that is most likely to be the most accurate when initiating the attack. However, as it is illegal to transmit forged GNSS messages, it is difficult to determine a cost associated with

setting up such an experiment. It is also challenging to determine an associated cost to the theoretical calculation. This is because it requires substantial knowledge to accurately determine the coverage theoretically. The last resource alternative utilizes an open-source software solution, which is the simplest and is the most likely alternative to be used by a threat agent group with limited capabilities. An example of such a solution is the one developed by Silicon Labs [Lab17]. The tool estimates coverage based on, among other things, field measurements performed by the company and requires only TX output power, TX antenna gain, RX sensitivity, RX antenna gain, and frequency bands as parameters.

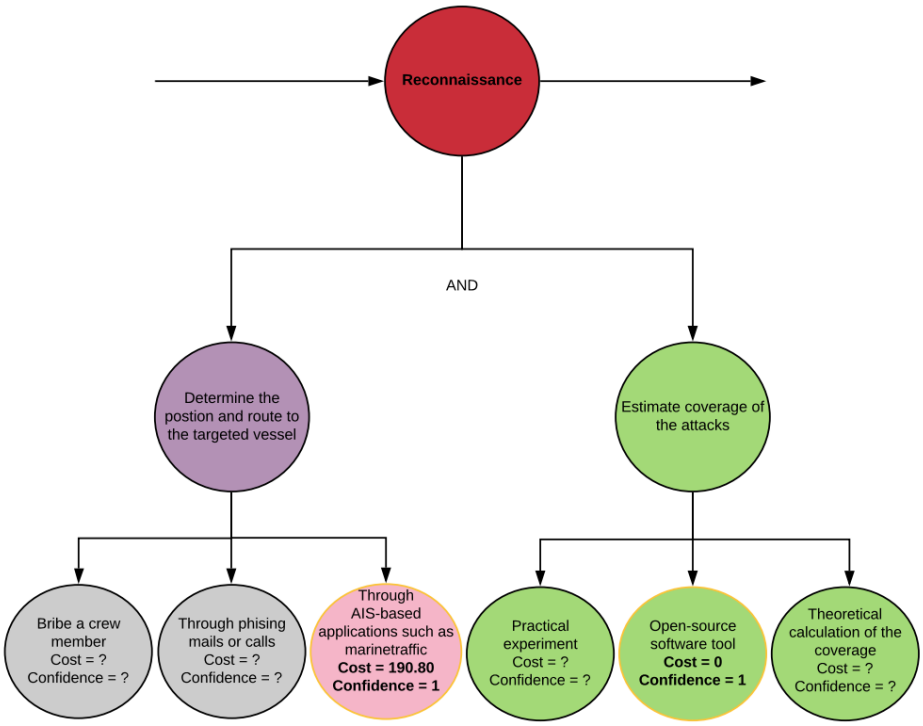


Figure 6.2: GNSS: Reconnaissance Stage

Weaponization

The weaponization stage couple an exploit with a deliverable payload. The exploited vulnerability, in the case of GNSS, is the lack of encryption and authentication for users of the system, excluding military personnel. By generating signals that appear legitimate, GNSS receivers may be lured to believe that the forged signals are legitimate, and use the forged signals for Positioning, Navigation, and Timing (PNT) services. However, to forge GNSS signals, a GNSS signal simulator is necessary.

Three potential methods were considered. The first method consists of utilizing a GNSS simulator, which is a tool used to test receivers before introducing the receivers to the market. The cost of a GNSS simulator was, in many cases, not listed and required to request a quote to get an estimate. However, a source from 2013 priced the GPS simulators to 47 500$ and upwards [Cre13]. This indicates that such equipment is expensive, even though those prices might have fallen a considerable amount since 2013. Nevertheless, as few sources were identified, the cost remains uncertain. The second option is to use open-source software such as the gps-sdr-sim in combination with an SDR. Even though the open-source software had some guidelines, modifications were necessary, and the cost is estimated between 250$ and 2000$. The cost is based on the necessary time and effort needed, where one hour of work is assumed to be worth 20$. The last option identified is writing specialized software similar to the open-source software. The cost required to finalize this task is, however, uncertain.

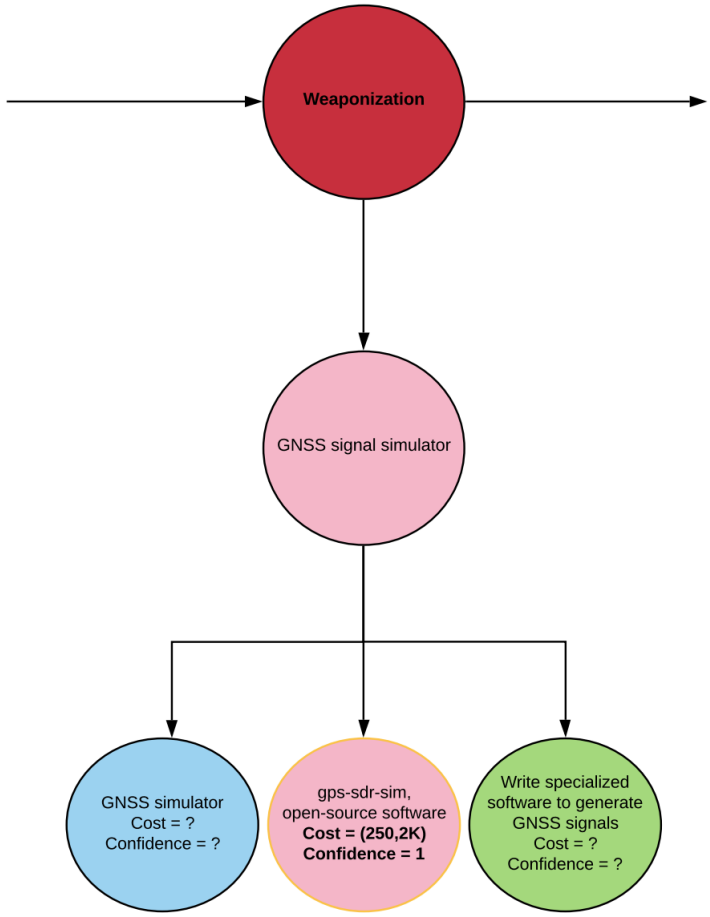


Figure 6.3: GNSS: Weaponization Stage

Delivery

To be able to achieve the desired outcome when delivering the payload, three resources are required to be fulfilled.

Firstly, a jamming attack is necessary. By jamming the signals, the receivers will lose their current lock onto the satellites and will start searching for new satellites. As seen in Figure 6.4, four resource alternatives were identified. The first alternative consists of a specialized GNSS jamming software in combination with an SDR. The second alternative includes acquiring a jammer which can be easily bought online. The range of jammers varies from a couple of meters to over 1000 meters and is highly related to the product's price [Jam]. The third resource alternative consists of a physical object acting as a jamming tool to disrupt the signal tracking. This alternative requires someone onboard the vessel to place the object over the antenna and afterward removing it. The resource alternative has a cost highly dependent on the person at hand. Lastly, natural terrain such as mountains can be used to disrupt the tracking and is free of cost. However, uncertainty regarding whether the natural terrain breaks the signal tracking or not may prevent this method from being used.

Secondly, the distance to the target needs to be determined. This is to ensure that the target is within the coverage of the attack. Radar, Laser-based rangefinders, and positional data obtained through AIS have been identified as potential alternatives. The price ranges that have been determined by using the following sources as the base for the estimates: Radar [1] [2], Laser-based rangefinder [3] [4], AIS receiver/transceiver [5] [6], and AIS antenna [7] [8] [9].

Lastly, an adversary needs to ensure that the signals are transmitted within the transmission range of the attack. This can be ensured by being onboard the targeted vessel, have a vessel following the target, following the target using a helicopter, or by being on a nearby coast. The cost associated with the resource alternatives is quite uncertain, except for the resource alternative where the adversary is on a nearby coast. A cost has, nevertheless, been associated with the alternative where an adversary uses a vessel to follow the target, as it is assumed the most likely alternative.

[1] https://ctmarine.no/butikk/kartplotter-og-multiskjermer/garmin/radar-3
[2] https://www.thegpsstore.com/Radar-C16.aspx
[3] https://www.amazon.com/Laser-Rangefinders/b?ie=UTF8&node=162019011
[4] https://www.bhphotovideo.com/c/buy/laser-rangefinders/ci/37565
[5] https://shop.marinetraffic.com/ais-transponders.html
[6] https://www.milltechmarine.com/AIS-Receivers_c_13.html
[7] https://www.quark-elec.com/product/qk-as02-149-vhf-antenna/
[8] https://shop.marinetraffic.com/ais-antennas.html
[9] https://www.amazon.com/slp/ais-antenna/z8a8f383rfm9667

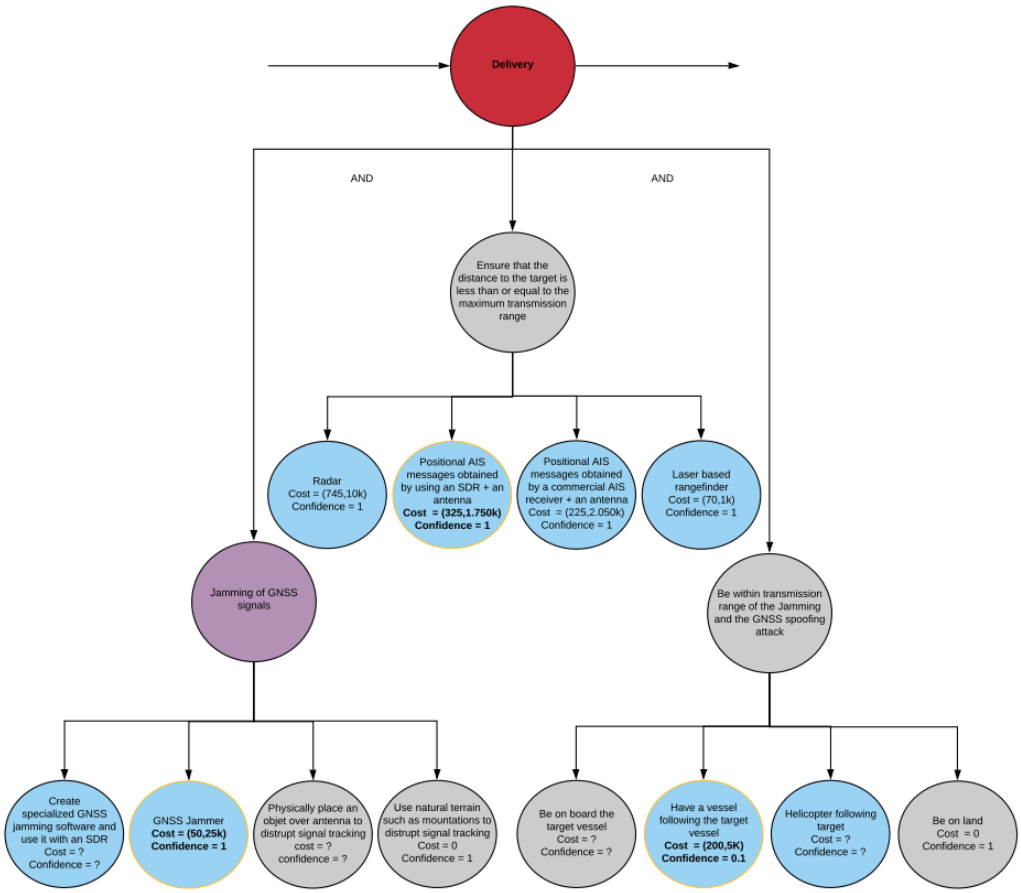


Figure 6.4: GNSS: Delivery Stage

Exploitation

The vulnerability that is being exploited is the lack of encryption and authentication to thwart modification and generation of GNSS messages. No resource alternative is necessary to obtain the resource as it is a fundamental problem with the system.

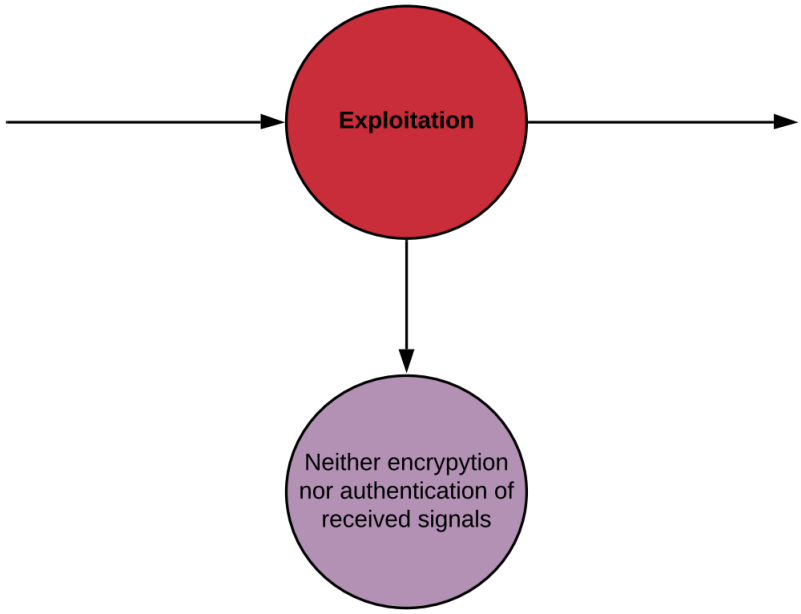


Figure 6.5: GNSS: Exploitation Stage

Installation

The installation stage consists of installing all prerequisite software and acquiring the necessary hardware to initiate the desired attack. As seen in Figure 6.6, four resources are deemed necessary in this stage. Hardware components capable of transmitting GNSS signals, a sufficient computer, an antenna, and prerequisite software are required and have been assigned an associated cost and a confidence level.

Most GNSS antennas are optimized to receive GNSS signals. It is, therefore, likely that the antennas designed for receiving GNSS signals are not suited for transmitting fake GNSS signals. It was difficult finding sources that sold antennas designed to transmit GNSS signals. Thus, a confidence of 0.5 was given to the estimate. In the scenario utilizing a GNSS simulator, the cost is set to 0 for the hardware component, as the cost was considered in the weaponization stage. Additionally, GNU radio is not required when using a GNSS simulator. However, the cost will not be affected by this resource as it has a cost of 0.

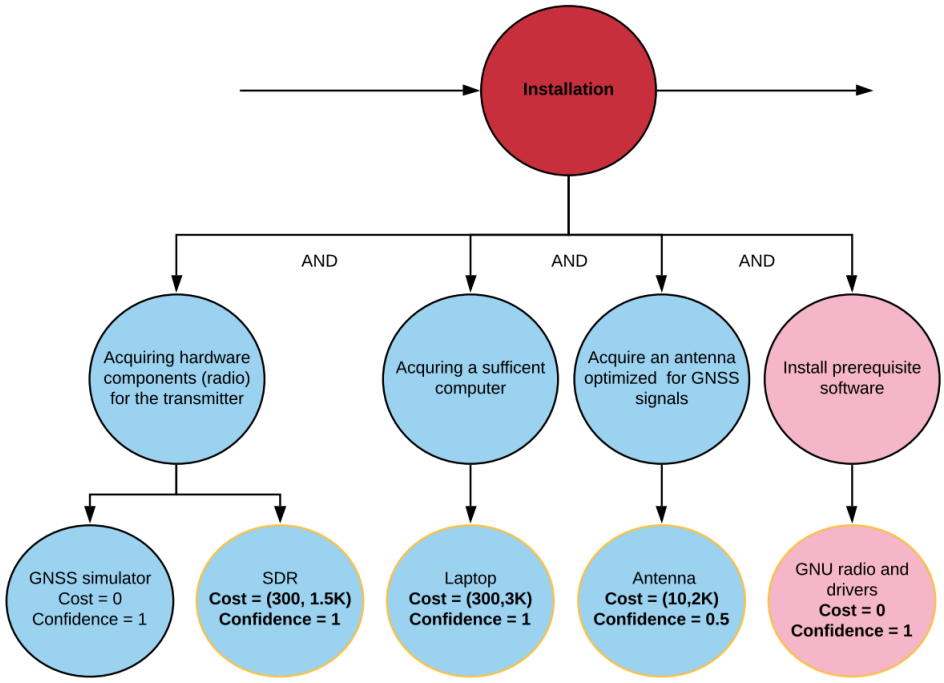


Figure 6.6: GNSS: Installation Stage

Command and Control

The intrusion kill chain is, as described in section 3.3, an Intelligence-Driven Computer Network Defense model. The model identifies the typical steps in a network-based attack. However, the model does not fit all types of cyberattacks, and is rather optimized for attacks where remote access is an important milestone for the adversary. This is not the case for AIS- or GNSS-based attacks, as remote access is not necessary to achieve the goal of the attack. Consequently, this stage has been left out for both the GNSS attack and the AIS attack in section 6.1.2.

Actions on Objective

To be able to mitigate the possibility of detection, it is important to forge a course that deviates slightly from the real course. A small deviation in the course will consequently make it harder to detect for the deck officers onboard the vessel. The adversaries have to identify the course of the target to be capable of forging a course that slightly deviate. The information may be obtained through AIS messages, by radar, or by using a laser-based rangefinder. However, no additional resource alternatives are necessary as the equipment necessary to identify the course and speed have already been considered in the delivery stage.

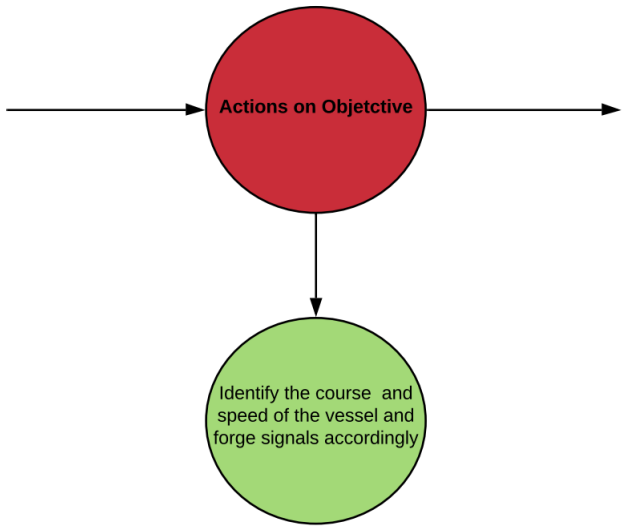


Figure 6.7: GNSS: Actions on Objective stage

6.1.2 AIS-based attacks

AIS-based attacks follow a similar procedure to GNSS-based spoofing attacks where a great amount of hardware and information are necessary for both classes of attacks. Consequently, several stages will not be further explained as it was done in the previous section 6.1.1.

Reconnaissance

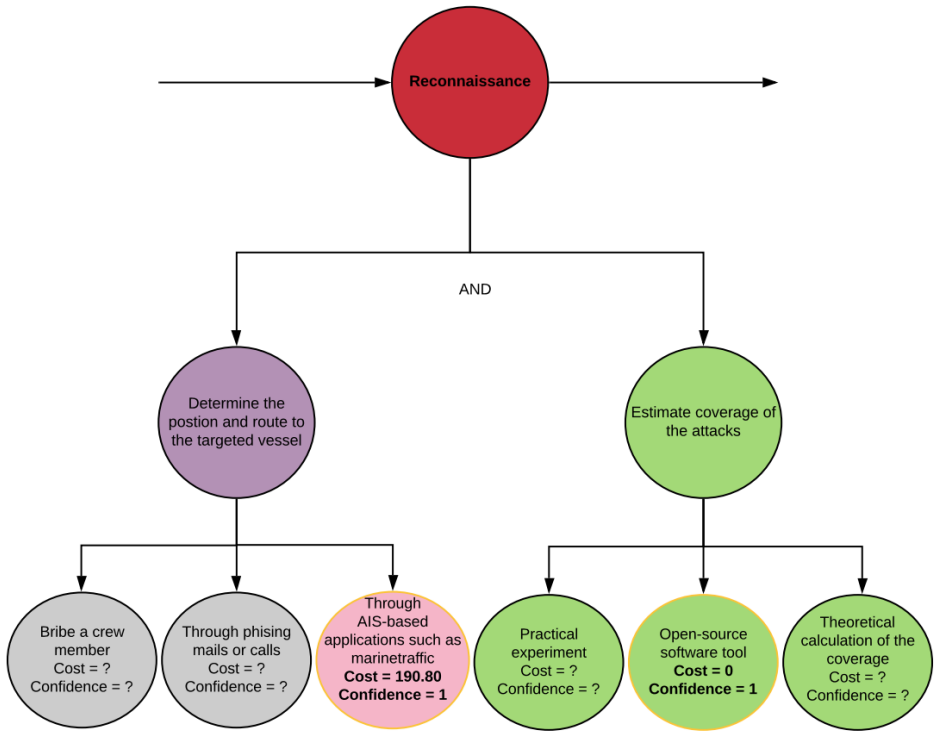


Figure 6.8: AIS: Reconnaissance Stage

Weaponization

An AIS signal simulator is necessary to generate forged AIS messages. Such messages can be generated by using the open-source software AISTX developed by Trendmicro, or by writing a specialized custom software. The cost associated with the open-source software is a result of the expected amount of time and effort, where one hour of work is considered to be worth 20$.

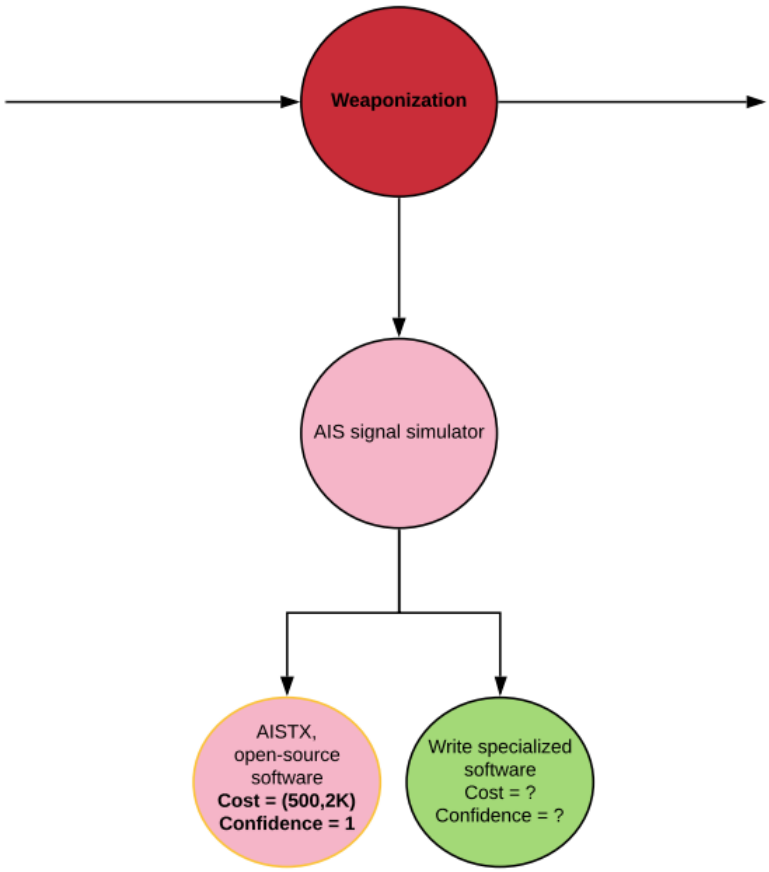


Figure 6.9: AIS: Weaponization Stage

Delivery

To deliver the malicious payload, being within the transmission range is the only necessary requirement in the delivery stage.

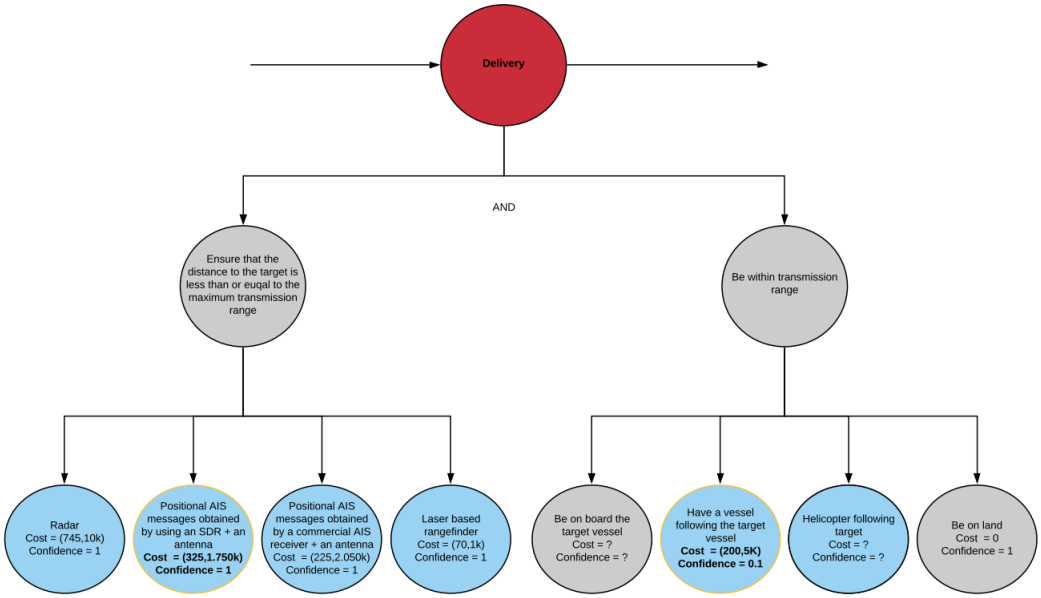


Figure 6.10: AIS: Delivery Stage

Exploitation

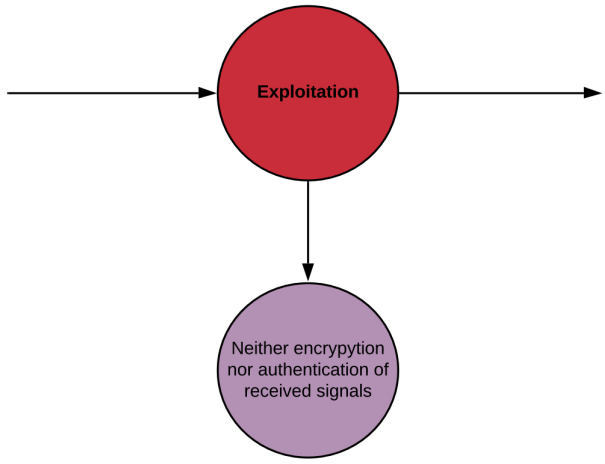


Figure 6.11: AIS: Exploitation Stage

Installation

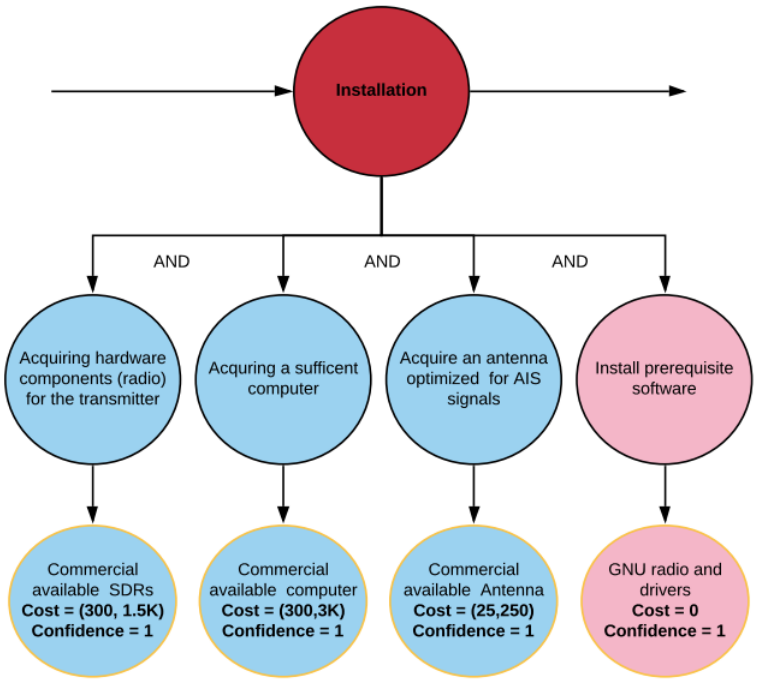


Figure 6.12: AIS: Installation Stage

Actions on Objective

As with GNSS-based spoofing attacks, AIS-based attacks need to identify the course and speed of the target. This ensures that the attack is optimized based on the victim's route.

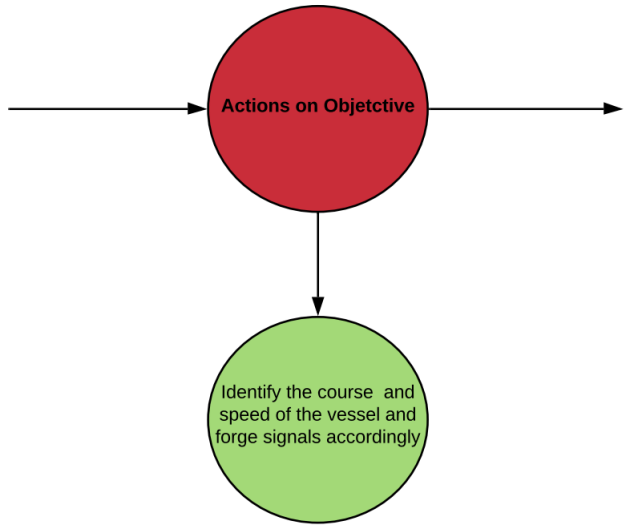


Figure 6.13: AIS: Actions on Objective stage

6.1.3 Estimation of Cost

Based on the equation for min cost (3.2), max cost (3.3), and confidence (3.4), a cost estimate has been calculated for each of the attack classes. As previously mentioned, it is important to note that the resource alternatives with the golden circles are the chosen alternatives for the estimate. Additionally, the cost of two SDRs have been included (one in the delivery stage and one in the installation stage) as one would act as a transmitter and one as an AIS receiver. This is, however, not always necessary as some SDRs can act as a transmitter and receiver simultaneously.

Furthermore, the maximum price of equipment such as computers and SDRs can, in some cases, be costly. However, more costly equipment may, in some cases, offer the same utility as cheaper equipment. Thus, the maximum cost of the equipment represents the maximum price, where the equipment is assumed to give a considerable advantage over more affordable equipment. This was chosen to narrow down the cost range, which otherwise would be extremely wide.

Additionally, the cost related to buying a signal amplifier has been excluded even though it is necessary if the transmission range of the SDR is insufficient. However, since it is not strictly necessary, it was left out of the equation.

GNSS spoofing attack (re-acquisition)

Reconnaissance [min, max, confidence] = [190.80, 190.80, 1]

Weaponization [min, max, confidence] = [250, 2000, 1]

Delivery [min, max, confidence] = [575, 31 750, 0.1]

Exploitation [min, max, confidence] = [0, 0, 1]

Installation [min, max, confidence] = [610, 6500, 0.5]

Command and Control [min, max, confidence] = Left out

Actions on Objective [min, max, confidence] = [0, 0, 1]

Total Cost [min, max, confidence] = [1625.8, 40440.8, 0.05]

AIS-based attacks

Reconnaissance [min, max, confidence] = [190.80, 190.80, 1]

Weaponization [min, max, confidence] = [500, 2000, 1]

Delivery [min, max, confidence] = [525, 6750, 0.1]

Exploitation [min, max, confidence] = [0, 0, 1]

Installation [min, max, confidence] = [625, 4750, 1]

Command and Control [min, max, confidence] = Left out

Actions on Objective [min, max, confidence] = [0, 0, 1]

Total Cost [min, max, confidence] = [1840.8, 13690.8, 0.1]

6.1.4 Discussion

Analysis of the estimates

The model constructed for both the AIS and GNSS are not fully completed, as several resource alternatives have yet not been identified. This resulted in a strategy where a set of valid resource alternatives were chosen to estimate a cost range for the attacks. However, by excluding several resource alternatives, a less comprehensive picture of the cost is made. Optimally, to identify the full cost range, the resource alternative with the lowest min cost and the resource alternative with the highest max cost that both have the same parent node should be combined for each resource node. A full cost range makes it more clear what the absolute minimum and maximum cost of such attacks are.

Furthermore, a full cost range makes it easier to determine which threat agents groups that have the capacity executes such attacks. On the contrary, by specifically choosing a set of resource alternatives that are deemed the most likely, the resulting cost range can be less extensive compared to a full cost range. However, smaller cost range makes it easier to pinpoint the particular attack to a particular threat agent group rather than several potential groups, which may be the case for a full cost range. By narrowing down the scope, countermeasures and mitigation techniques may be directed towards a small group of agents, which makes it less costly.

The stages in the intrusion kill chain have been clearly divided to highlight the cost and confidence of each stage. The separation makes it easier to identify the cost that is required at a specific stage, and the confidence associated with the stage. In the case of GNSS- and AIS-based attacks, it is clear that the delivery

stage is the stage with the highest amount of uncertainty and should, as a result, be investigated further. At the same time, most of the other stages have confidence close to 1 and indicate that the costs associated with the stages are likely to be accurate. Nevertheless, the total cost is profoundly affected by the low confidence associated with the delivery stage, which gives a low overall confidence.

Limitations of the model

The Resource Cost Estimate Model suffers from some clear limitations. First and foremost, it is not clear how to set the confidence level. This makes the confidence level subject to personal opinions, which makes replication of previous models harder. To be able to mitigate this problem, a clear guideline on how to set the confidence level should be created.

The model identifies potential resource alternatives, but does not take into consideration which alternative is most likely to succeed or which is the most likely to be used. Thus, attacks that are possible in theory, but rather infeasible in practice may be used as a base for the estimate. As a result, the range of the estimate may become more extensive than the cost range would be in practice. However, it is not always clear which resource alternatives are likely to be used or not, and which resource alternatives are likely to be successful.

Cost related to hardware and labor is dependent on several factors. The cost related to hardware devices and labor changes in many cases based on location, and is a factor that needs to be considered. Additionally, labor cost is also dependent on factors such as the occupation to the adversary. Some tasks can be completed by a wide range of people with different background. Depending on the background, a person may evaluate one hour of work or one line of code differently from a person with another background. In the Weaponization stage for both the AIS and GNSS attack, an hour of work is valued at 20$. This estimate is, however, not necessarily accurate as a script kiddie and a software engineer would evaluate one hour of work quite differently. The estimate is, therefore, rather an estimate of the amount of time necessary to make the software work. It needs to be adjusted depending on the threat agent group that is suspected of executing the attack when creating a model.

Chapter 7
Interview Findings

This chapter presents the findings from the eight interviews that were held. The findings are categorized by the interviewees in relation to the three themes identified in chapter 3 under section 3.5.1. Table 7.1 illustrates the interviewees and their respective sections, where the findings are described. It is important to note that to be able to preserve the anonymity of the interviewees, no personal data was recorded during the interviews. Furthermore, no details that could compromise the interviewees' anonymity have been included within this master thesis.

	Section 7.2	**Section 7.3**	**Section 7.4**
	Maritime pilots	**Deck officers**	**Maritime traffic leaders**
Title	Maritime Pilot	Captain	Maritime traffic leader
Experience	22 years	23 years	14 years
Title	Maritime Pilot	Captain	
Experience	9 years	4 years	
Title	Maritime pilot	Chief mate	
Experience	7 years	2 weeks	
Title		Second mate	
Experience		5 years	

Table 7.1: Interviewees' experience and current title

7.1 Industrial Context

Maritime Pilots and Traffic Leaders

The Norwegian Coastal Administration (NCA), founded in 1974 [SM], is an agency of the Norwegian Ministry of Transport and Communications and is responsible for the water transport industry along the Norwegian coast. The agency is responsible for providing services related to maritime safety, maritime infrastructure, transport planning, and more. Two of the most critical services that the agency offers are piloting services and Vessel Traffic Service (VTS) [SM19].

Pilot services aim to safeguard traffic at sea and mitigate the likelihood of navigation-related incidents. This is achieved by offering marine pilots with adequate qualifications for safe navigation to vessels operating in specific geographical areas in Norwegian waters that are considered critical. A Port is a typical area considered as critical and offers pilot services to help guide vessels to and from the port. Marine pilots typically have a lot of knowledge of the local waters they operate in, which they have gradually obtained after sailing the same waters for several years. This gives the marine pilots an advantage over deck officers onboard the vessels, which most likely are not as familiar with the waters as the marine pilots. Consequently, by hiring a marine pilot for guidance, the likelihood for an incident to occur decreases.

Once a vessel requests a pilot service, a marine pilot needs to equip himself with tools to aid in navigation and board the vessel requesting the service. Typically, the tool known as the pilot's Portable Pilot Unit (PPU) is brought to aid the pilot in safe navigation. The tool consists of a laptop displaying electronic charts that incorporate information obtained by a range of systems such as GNSS and AIS [Ass16]. After boarding the vessel, the vessel can start to navigate to the desired location with the guidance of the pilot. The pilot then returns back to his station, where he waits for a new vessel to request his service. Pilot services are, however, not always optional, as according to Norwegian law, vessels with a length of 70 meters or more are subject to Compulsory Pilotage when operating in specified areas [Adm11a]. The requirement of Compulsory Pilotage can either be met by hiring a marine pilot or by the use of a Pilot Exemption Certificate (PEC). The PEC can be issued to deck officers and ensures that the holder is qualified to sail in specific fairways or areas with the specified vessel, without a pilot [Adma].

VTS aims to prevent incidents and accidents by monitoring and regulate vessels in specified areas along the Norwegian coast. Maritime Traffic Leaders are stationed at VTS centers and are responsible for protecting the environment and ensuring efficient and safe navigation of vessels within a VTS area, by offering different types of VTS services such as guidance [Admb]. The Traffic Leaders are stationary, and all services are given remotely. By using equipment such as AIS, radar, video cameras,

meteorological sensors, and SafeSeaNet Norway (SSNN) vessel reporting system, Maritime Traffic Leaders can get a solid overview of vessels inside regulated VTS areas. On the other hand, Maritime Traffic Leaders will have a less comprehensive overview outside the regulated areas, as radar and video cameras no longer covers the area. Nevertheless, AIS and SSNN are still available outside the regulated areas, as a result of the NCA's AIS chain along the Norwegian coast.

VTS offers three types of services [Adm11c]:

1. The Information Service (INS) provides information to help vessels make navigational decisions. Information provided by the VTS center can be anything from information on the current traffic situation, to Meteorological information.

2. Navigation Assistance Service (NAS) is a service that is either provided at the request of a vessel or when the Maritime Traffic Leader deems it necessary due to irregularities in how the vessel operates. The duration of the service is pre-agreed between the vessel and the Maritime traffic Leader, before the service is provided. After initiating the service, the VTS center can offer advice such as the recommended course to the next waypoint, which is an intermediate point on the route.

3. Traffic Organisation (TOS) provides information, advice, and instructions to prevent dangerous situations from arising and is a service used to ensure efficient and safe navigation through the VTS regulated area. The service can provide instructions such as specifying the order vessels shall sail, or whether vessels should use special fairways.

There are currently five VTS centers along the Norwegian coast that constantly monitors the traffic.

Captains, Chief Mates (C/Os), and Second Mates (2/Os)

The captain is the highest-ranked official and holds the final responsibility and command onboard a vessel. The captain is responsible for the crew, passengers, cargo, equipment, navigation, and safety. To serve as a captain on a commercial vessel of any type and size, the certificate "Deck Officer D1" is required. The qualification standards for certificates are universally set by the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) [IMOb].

C/O is the second in command following the captain, which means taking over the command if the captain is unable to carry out his duty. The C/Os is the head of the deck department of his vessel and responsible for the entire cargo operation,

which includes loading, discharging, cargo planning, and cargo handling. He is also responsible for the safety of the vessel both in port and at sea. To serve as a C/O, the certificate "Deck Officer D2" is required.

2/O is a member of the deck department, together with the captain and C/O. A vessel usually consists of at least a captain, a C/O, and 2-3 C/Os. The second mate is responsible for the navigational equipment as well as assisting the captain and C/O in their tasks. To serve as a 2/O on any vessel, the certificate "Deck Officer D4" is required.

7.2 Marine pilots

This section presents the findings from the interviews conducted with three marine pilots.

AIS and GNSS dependency

As described in table 7.1, the marine pilots have 7, 9, and 22 years experience in their current position. They were all located at different stations around in Norway. Despite the informants being located at different locations with varying amounts of experience as a pilot, they agreed on the main reference points used for navigation when sailing. Radar, ECDIS or traditional nautical maps, and lastly, their vision was considered as the essential tools necessary to navigate correctly.

The pilots considered AIS as an excellent tool for planning, as waypoints may be set depending on upcoming traffic. Additionally, AIS is used as a tool to plan appointed missions efficiently, as it becomes easier to predict when a vessel requesting pilot services arrives. Consequently, a pilot may decide to go bed either earlier or later, depending on the estimated Time of Arrival (ToA) of a vessel. The pilots, however, did not consider AIS as a critical tool in regards to navigation, and would not hesitate to complete a mission with a malfunctioned AIS system as long other conditions were considered normal. Nonetheless, under certain conditions such as when the radar is not functional, and the visibility is poor, increased trust in the AIS system is necessary to achieve good situational awareness.

GNSS is a valuable tool that can help a vessel obtaining its exact position and is typically used in combination with electronic charts. The pilots deemed the positional data obtained from GNSS systems advantageous to determine the position of the vessel quickly. However, under normal conditions, none of the pilots would consider the positional data obtained by GNSS systems to be crucial to a point where it would be impossible to complete a mission. All three pilots also pointed out that all pilots are trained to navigate without any navigational systems. Furthermore, their knowledge of the local waters makes them better equipped for conditions with a

limited amount of navigational systems. Consequently, in situations where incorrect AIS and GNSS data are obtained should not affect the navigation to the pilot.

Awareness and preparedness

In general, the interviewed pilots distrusted electronic systems and preferred to navigate with their eyesight in combination with the systems. The distrust stemmed from mainly two reasons. Firstly, the pilots were skeptical of information received from other sources than the vessel they were currently operating, as they do not have control over the systems outside of the vessel. Thus, messages obtained through AIS and GNSS were considered more likely to be incorrect compared to information obtained by radar. Secondly, some systems such as AIS and GNSS are additionally prone to errors, which further reduces the general trust in the systems.

The interviewed pilots were all familiar with incorrect AIS data as a result of wrong user input, such as positional AIS messages indicating an incorrect heading. Vessels have to input several parameters manually, such as destination before a voyage, and are the reason for user-based errors. Nevertheless, most of the information sent by AIS is not accessible by a regular user and can not, therefore, be modified manually. Thus, a regular user can not modify AIS parameters such as the current position of the vessel, as this is automatically transmitted. The awareness regarding attacks where forged messages are transmitted was, however, nonexistent, as none of the interviewees knew it was possible to forge all the 27 AIS messages. None of the interviewees had ever experienced such an attack or heard it was possible to execute such an attack.

The interviewees were familiar with limitations and errors that may occur when using GNSS. They were also familiar with the reduced accuracy or the loss of signal that may occur when sailing in-between mountains. Consequently, all the interviewees were aware of the inconsistent position accuracy and did, therefore, trust the system completely. Additionally, they were aware of the potential risk of GNSS jamming. Two of the interviewees knew about the spoofing attacks that happened in the black sea in 2017 between June 22-24, as it was covered extensively in the media [GPS17]. As with AIS-based attacks, none of the interviewees had ever experienced a GNSS-based attack.

Even though some issues related to GNSS and AIS are known by the pilots, limited precautions and responses are prepared to handle attacks. One of the pilots explained that they are particularly trained to handle situations where the GNSS receivers are not working. However, the other pilots were not familiar with such training when asked whether the staff was trained to handle situations without AIS and GNSS services. Furthermore, no training regarding other potential attacks were disclosed by the interviewees. There is no official procedure regarding handling and

reporting such incidents. However, the interviewees stated that they would convey information about the irregularities up the chain of command if they noticed being under attack.

Potential outcomes of attacks

The interviewees had not experienced problems with GNSS or AIS other arbitrary errors or users mistakes. Thus, it was hard for the interviewees to imagine the worst possible outcome of an attack. Nevertheless, the pilots were convinced that under normal conditions with good visibility and operating radars, most attacks related to AIS and GNSS should not result in a devastating outcome. When asked whether spoofed vessels would cause any concerns or problems, the pilots replied that as long they could not see the vessel by using their eyes or on the radar, the message would be disregarded, and the voyage would continue as normal. However, they explained that this applies under normal conditions. The response to a spoofed vessel would likely change under conditions where visibility and the effect of radars are reduced.

When asked about the response to a SART spoof attack, the pilots admitted that such a message could not be overlooked and would need further investigation to ensure that the message was illegitimate. However, the pilots were uncertain to what extent this attack would be damaging to the vessel and deemed it unlikely that significant damage would occur as a result.

Under certain conditions, the pilots agreed that in a worst-case scenario, the vessel they were operating could run aground. However, they were uncertain how such an event would unfold, and what the required steps would be to lure them to an extent where a vessel could run aground.

7.3 Deck officers

This section presents the findings from the interviews with the four deck officers.

AIS and GNSS dependency

As described in table 7.1, we interviewed two captains with 23 and 4 years experience in the position, one recently promoted chief mate with only 2 weeks experience, and one second mate with five years experience. Despite a wide range of experience, every deck officer was familiar with navigational equipment such as AIS, GNSS, ECDIS, and radar. As with the marine pilots, they considered their vision to be the most important asset when navigating.

The deck officers considered AIS as a helpful tool to gain information about other vessels nearby. They used information such as position, course, and destination

of other vessels to get an overview in trafficked waters. None of the deck officers considered AIS as a critical system as they did not use it for navigation nor collision avoidance. If the system experienced arbitrary errors or downtime during a voyage, it would not impact the voyage. The deck officers with less experience seemed to use the system to a greater extent compared to the more experienced deck officers. Some of the more experienced deck officers explained that they only used AIS a couple of times during a voyage if information such as ETA were to change. The less experienced deck officers would monitor AIS throughout a voyage.

According to the deck officers interviewed, GNSS is the most important tool to obtain the exact position of the vessel. Some of the deck officers considered GNSS as a critical system. A loss of GNSS signals in open waters would require to use a sextant to regain the position of the vessel. However, closer to shore, the position is calculated by cross-checking information from radar with the vision. Further, the deck officers explained that they have training and procedures for navigating in emergencies without electronic equipment in bad weather conditions. Therefore, loss of GNSS would not interrupt a vessel's voyage to its destination.

Awareness and preparedness

As with the maritime pilots, the deck officers were somewhat skeptical of electronic systems, and distrusted the systems for the same reasons as described in section 7.2. Therefore, to avoid false information, the information obtained from one system is always cross-checked with another system to make sure that it is correct.

The deck officers were also familiar and had experienced incorrect AIS messages due to incorrect user input in static data such as destination, dimensions, and Time of Arrival (ToA). The deck officers with more experience were not aware of attacks with malicious intent created by forged AIS messages. However, the more recently educated deck officers had some knowledge about forged AIS messages. Nevertheless, it was only limited to the existence of the messages. They were unaware of which messages could be forged or which types of attacks they could result in. The deck officers with some knowledge about forged AIS messages explained that they had learned about it in training programs, and at the maritime school.

The deck officers were well aware of the limitations and errors that can occur when using a GNSS. They explained that a loss of signal could happen when sailing close to surrounding terrain such as mountains. However, the deck officers clarified that this was usually a bigger problem for maritime pilots as they usually overtake the command when sailing close to the shore. Further, the variations in position accuracy was another reason why they did not trust GNSS 100%. The deck officers were also aware of GNSS jamming, and one of them had experienced their GNSS signal being actively jammed during sailing. This event took place during the Iran-Iraq war when

GNSS was globally unstable to avoid reviling the position of war ships, according to the interviewee. Other than this particular experience, none of the deck officers had experienced a GNSS-based attack.

As with the maritime pilots, the deck officers were familiar with some vulnerabilities related to AIS and GNSS. As previously mentioned, the deck officers had training and procedures to navigate without the help of electronic systems. However, there were no procedures regarding attacks with malicious intent.

Potential outcome of attacks

When asked about the outcome of a successful attack against AIS and/or GNSS, some deck officers had difficulty imagining catastrophic consequences. The deck officers explained that cross-checking information between different systems is common practice, and argued that false information would, therefore, be detected. Due to duplicates of several systems onboard large vessels such as two radars, two GPS receivers (AIS has its own GPS receiver), and backup communication systems, the deck officers, did not find it problematic if one or more system were attacked. Even in the unlikely scenario where every system is taken down, their ability to navigate without electronic systems by using a sextant, maps, and their vision would avoid dangerous situations, according to the deck officers.

As with the maritime pilots, the deck officers considered SART spoofing attacks problematic as SART messages could not be overlooked. However, the deck officers would check other communication systems for emergency messages before steering the vessel off course, especially in waters known for piracy. According to the deck officers, a vessel does not have to assist in an emergency if it put themselves at risk. Therefore, the deck officers found it unlikely that SART spoofing attacks could create dangerous situations.

The deck officers agreed with the maritime pilots, under certain conditions, an attack on their navigation systems could, in theory, lead to a vessel running aground. However, they were not able to give specific examples of such conditions.

7.4 Maritime Traffic Leader

This section represents the findings from the interview with a maritime traffic leader.

AIS and GNSS dependency

The maritime traffic leader interviewed has mainly the three systems, radar, video cameras, and AIS to his disposition when giving navigational advice or commands. The primary purpose of the video cameras is to identify whether an area has good

or poor visibility, which can help vessels prepare for the particular condition in the area. The interviewee used radar and AIS for similar purposes, and they are the main tools to identify a vessel's position and its course. However, the radars that the traffic leaders have access to do not cover the regulated VTS area completely. Outside of the radar covered areas, AIS is the only reliable tool to identify vessels' position and course.

The dependency in AIS has gradually increased throughout the last decades and is a more critical system than ever before, according to the traffic leader. Prior to AIS, radar was the main system to identify vessels within regulated VTS areas. However, as more vessels utilize AIS and as it has become mandatory by law for certain vessels, AIS has gradually become more important to the traffic leaders. Furthermore, according to the interviewee, fewer errors and incorrect data are obtained compared to previous years. As a consequence, the received AIS data is more trustworthy. Nevertheless, the interviewee would still consider radar more credible compared to AIS if contradictory information were received by the systems. The reasoning behind the interviewee's choice is that the radars are not dependent on other entities than themselves. Additionally, the interviewee has rarely experienced inaccurate or misleading data obtained from the radar, which has lead to an increased trust in the system.

VTS centers do not use first-hand data obtained through the use of a GNSS and was therefore not discussed in great detail with the interviewee.

Awareness and preparedness

The traffic leader interviewed was aware of some of the limitations related to using AIS. Incorrect and inadequate data have been obtained quite a few times. On several occasions, the interviewee had received AIS messages stating that vessels are located at land. Inaccurate GNSS data is the reason behind the misleading AIS message. The interviewee had also experienced receiving AIS messages from a non-existing vessel. This is typically a manufacturer transmitting AIS signals when testing equipment, according to the interviewee.

According to the interviewee, traffic leaders receive limited training regarding AIS. Some limitations within AIS is taught throughout this training. However, there is no training related to the potential attacks that may occur. Consequently, an increased understanding of the limitations and weaknesses of the system have to be obtained through years of experience. In case of an incident or when an anomaly is detected, a report is constructed and sent to the technicians working within the VTS center. The technicians have a greater technical understanding of how AIS works and try to identify the reason behind the incident and to see whether a malicious actor was behind it.

According to the interviewee, a filtration mechanism is applied to the data obtained by the NCA's AIS chain. The purpose of the filtration mechanism is to remove bad and illegitimate data, and therefore make the data more reliable. However, the traffic leader could not explain in detail how it worked.

Potential outcomes of attacks

The interviewee states that the potential outcomes of the attacks depend on what type of attack is executed and whether backup systems are available. Generally, the safety of the vessels within the regulated area will be reduced as a consequence of an attack. However, if the adversary transmits malicious positional AIS messages within an area covered by radar, the interviewee could verify this message with the radar system. Thus, it is easy to identify that there is something wrong with the data obtained. The interviewee states that if such a case occurs, the safety of the vessels would not be considerably reduced. On the other hand, if no radar is available and such an attack occurs, the safety of the vessels would be significantly reduced as the advice given would be based on malicious data.

According to the interviewee, all vessels over 24 meters are obliged to report to the VTS center when they are using a VTS regulated area. This information, in combination with the SSNN vessel reporting system, gives an indication to the traffic leaders whether vessels identified by AIS are supposed to be in the area, and can be used as a tool to help detect malicious positional AIS messages.

Chapter 8
Discussion

The following chapter will address the research questions that have been defined and discuss the results that have been obtained. Furthermore, throughout this chapter, the weaknesses and strengths of the methods used will be further highlighted as the research questions are being addressed.

8.1 Necessary resources and the feasibility of AIS- and GNSS-based attacks

RQ1: What kind of resources are necessary to launch successful AIS- and GNSS-based attacks in the maritime sector, and how feasible are such attacks?

The resources necessary to initiate AIS- and GNSS-based attacks on vessels in the maritime industry have been identified by using the Resource Cost Estimate Model. Additionally, a range of AIS- and GNSS-based attacks have been executed successfully to determine the required knowledge and effort to execute such attacks, as shown in chapter 4 and 5.

As shown in chapter 4 and 5, the process to generate fake GNSS and AIS signals are quite feasible and requires only an SDR that is compatible with the respective software and a laptop. However, it became evident that the guidelines posted alongside the software worked in varying degrees depending on which SDR used, which lead to several necessary alterations. Familiarity with building and configuring software in combination with a high degree of technical understanding within the field was, as a result, helpful when investing the problems that occurred. Having access to several SDRs made it easier to identify and solve the problems. Furthermore, at the respective repositories, several issues have been created, which were valuable when obstacles were encountered. This master thesis will even further reduce the complexity to build and generate fake GNSS and AIS data when it is published. As a consequence, adversaries with little knowledge within the field can recreate the attacks conducted if similar equipment is used.

After having the ability to generate GNSS and AIS signals, an adversary needs to ensure that the target is within the range of the attack. Thus, the coverage of the attack needs to be determined, either with a practical experiment or theoretically. The cost estimate produced in chapter 6 assumes that the adversary uses a software tool to identify the transmitting range of the attack [Lab17]. By using a software tool to identify the transmitting range, it is easy for an adversary to estimate the coverage of the attack. However, the tool might be inaccurate, which may compromise the attack if the target is outside the actual transmission range when the attack is executed. An alternative method would be to estimate the distance based on theoretical equations. However, the coverage of a transmitter depends on several factors such as obstacles, humidity (may absorb RF energy), metal objects reflecting radio waves, and path loss. Thus, creating a suitable equation for a particular environment requires a considerable amount of knowledge of how RF transmission works.

The overall cost to execute such attacks is in a best-case scenario, not particularly high. If the steps in chapter 6 are followed, a cost of 1700$ is necessary to execute the attack. Nevertheless, it is some uncertainty associated with the estimate, especially related to how an adversary would deliver the payload. The adversary needs to stay within a certain range relative to the targeted vessel to be within the transmission range. There are several ways an adversary can pursuit the targeted to ensure being within the transmission range, but the method that was considered most likely was with a vessel. The price to rent a vessel is highly dependent on the location where the vessel is rented. Additionally, a different type or size may be required depending on whether the attack is taking place in rough or calm waters. Thus, it is hard to estimate an associated cost with high confidence in the delivery stage.

A part of research question 1 tries to investigate the resources that are necessary to launch a successful attack. However, when an attack is considered successful have not yet been discussed. In chapter 4 and 5, an attack is considered successful if a malicious message transmitted is accepted, and the targeted system responds as intended. However, in many cases, the adversary intends to execute attacks that also go unnoticed by the target operating the system. Hence, making it more likely that mistakes are being made, which could be desirable for the adversary. The interviews conducted highlight how many operators of navigational equipment do not inherently trust electronic systems such as those based on GNSS and AIS. Furthermore, errors and deviations commonly occur within the systems, which further decreases the trust in the systems. Thus, to lure the crew aboard the vessel, malicious data must be forged and delivered in a manner that does not arouse suspicion. However, this is something that is not emphasized to a great extent in chapter seven 6, where the costs of potential attacks were estimated. The estimate focuses rather on the cost necessary to launch such attacks in the simplest form where detection is more

likely. Consequently, if the attack is discovered or the data that are obtained seem suspicious, the severity will be drastically reduced, and the goal of the attack is likely not to be accomplished. Additionally, the cost estimate ranges that were calculated are likely to be to narrow for the attacks in more advanced forms, as more resources will be necessary to ensure that the attack goes unnoticed.

To summarize, only a limited amount of equipment, knowledge, and resources are required to launch simple AIS- and GNSS-based attacks. Thus, the executing of such attacks in a lab environment is quite feasible and could be manageable by a wide range of agents, given enough time. However, the ability to execute such attacks successfully on unknowingly vessels require significantly more knowledge, as coverage needs to be determined, and a stealthy attack needs to be crafted, making such attacks in practice less feasible for a wide range of agents.

8.2 Criticality of AIS and GNSS systems

RQ2: How critical are AIS and GNSS services for the industry?

Before the interviews, relevant literature related to the research question was studied and helped to form a basis for our opinion on the research question itself. Consequently, we considered AIS and GNSS as critical systems for every stakeholder in the maritime industry, as indicated by the literature. The term ”PlayStation-mode” was even introduced by Hareide et al. [HOM16] to describe deck officers' excessive trust in electronic navigation systems.

During each interview, the interviewee was asked about the criticality of AIS and GNSS. The results from chapter 7 shows that the deck officers and maritime pilots did not consider AIS as a critical system. The system status of AIS would not affect a vessel's voyage since it is not used for navigation. However, the maritime pilots use AIS to a greater extent compared to the deck officers by also using it for collision avoidance and ToA. During the interviews, it was never explained why the deck officers did not use AIS for collision avoidance when it is used daily by the maritime pilots. The areas operated by the deck officers and maritime pilots might affect the answer. The deck officers usually sail in open waters where the traffic is less dense. Therefore, they encounter fewer vessels during a voyage. Maritime pilots usually sail in trafficked areas where the course and speed of nearby vessels are important information to avoid, for instance, meeting oncoming vessels in a narrow canal. The situation was, however, different for the maritime traffic leaders. They considered AIS as more critical than ever before as AIS is one of the three central systems to monitor traffic at sea, especially in areas not covered by radar.

The interviewees interacting with GNSS considered it an essential tool to locate

their exact position. The word ”critical” was never defined during the interview, which led to inconsistent use of the word. The same fictitious situation was classified as critical and non-critical by two different stakeholders during the interview. However, if ”critical” is defined as not being able to complete a voyage, none of the stakeholders considered GNSS as critical. The stakeholders would complete their voyage by using other tools to locate their position, such as the help of a sextant and maps. However, it is worth noting that the sextant is not mandatory equipment by the Safety of Life at Sea (SOLAS) convention [SOL].

From the findings in chapter 7, it is clear that the criticality of AIS and GNSS varies from stakeholder to stakeholder. We believe the dependency of AIS and GNSS are less than the literature indicates mainly due to two reasons. Firstly, the maritime industry seems to trust radar to a very high degree as it is not dependent on other entities than itself and is, therefore, used as the main tool for collision avoidance. Secondly, deck officers and maritime pilots have great confidence in their abilities to operate a vessel without any electronic aids, as this is a apart of their education. From the interviews conducted, it seems like the loss of vision is more critical than malfunctions in both AIS and GNSS.

8.3 How prepared is the industry?

RQ3: How well prepared is the industry to handle incidents affecting navigational equipment dependent on AIS and GNSS services?

The overall awareness of vulnerabilities existing within AIS and GNSSs seems to be somewhat limited among system operators within the industry. As a consequence, it is challenging for the operators to grasp the extent of what types of attacks are possible. Chapter 7 highlights this assumption as the types of attacks known by the interviewees are primarily a result of personal experiences and training programs. These training programs do, however, not consider the fundamental vulnerabilities within the systems. Consequently, the preparedness of an operator, is mainly based on which training program the respective operators has gone through and experiences in the field. Thus, some operators are better equipped than others to handle malicious messages.

The training programs and the education the interviewees received seemed to contain some variation in regards to incident response and knowledge given about particular attacks. Some of the interviewees stated that specific training related to particular attacks were given, whereas most stated that no such training was given prior to obtaining their current role. It is unclear why the interviewees had such a different experience with their training. However, it is likely that the location and the year the training were given affect the experience. Nevertheless, education

and training in recent years have probably become more focused on such attacks as cybercrime has become an increasing problem in recent years.

Although some interviewees had received training on how to respond to particular attacks, a clear consensus was given by the interviewees when asked which protocol was followed to report such attacks. The consensus was that no such protocol existed. However, they all agreed that suspicious information would be reported in one way or another, typically up the chain of command.

The maritime traffic leader interviewed explained that a filtration mechanism is applied to the data obtained by the NCA's AIS chain. However, the traffic leader was not able to explain in great detail how it worked, but explained that it increases the reliability of the data obtained. An email thread was created with one of the senior engineers working at the VTS center to investigate this further. The senior engineer stated that the NCA ensures that the received AIS data are correct but were not sure how this was realized in practice. Thus, a new email thread was created with one of the senior engineers within the VTS center with a cybersecurity background. The senior engineer did, however, not reply to the emails that were sent, which makes it infeasible to evaluate whether the filtration mechanism actually would affect the attacks.

Nevertheless, the industry seems to prepare to a limited degree for AIS- and GNSS-based attacks, as the types of attacks, have had a small impact on the industry so far. However, the importance of safe navigation has steadily increased during the last century. As a response to the Titanic disaster, the Safety of Life at Sea (SOLAS) convention was adopted in 1914 with the primary objective of ensuring safe navigation by defining a set of minimum standards for the construction, equipment, and operation of vessels [IMOa]. The convention has been updated on numerous occasions since it was first adopted to maintain its relevance. Currently, GNSS receivers, AIS transponders, and one or in some cases, two radars are required for vessels over a specific size and passenger vessels regardless of any size [SOL]. Although the convention does not explicitly address GNSS and AIS attacks, a more robust system is created by defining a set of necessary equipment for vessels to use. Thus, more fallback systems are available if one is to fail or to produce misleading data, which makes disasters as a result of an attack less likely. It is reasonable to assume that the overall awareness within the industry will increase as cybersecurity is getting increasingly more attention. However, it is unlikely that countermeasures will be implemented overnight without a disastrous event, as implantation of countermeasures come with a substantial cost.

8.4 Potential outcome of AIS- and GNSS-based attacks

RQ4: What could be the potential outcome of AIS- and GNSS-based attacks?

From the findings in chapter 7, it is clear that seven out of eight interviewees had never experienced problems with GNSS or AIS other than arbitrary errors or user mistakes. The interviewees did, therefore, not seem to worry about the potential outcomes of attacks and had a hard time imagining worst-case scenarios.

From the interviews, it was clear that the maritime pilots and deck officers were very confident in their abilities to navigate a vessel even without electronic navigation systems. From the findings in chapter 7, it is reasonable to assume that the interviewees did not rely blindly on information obtained from AIS and GNSS due to wrong user input and arbitrary errors. Carrying out successful malicious attacks via AIS is, therefore, not straight forward. According to the interviews, a spoofed vessel appearing on AIS during normal conditions where the vision, GNSS, and radar are available would not cause any problems. Considering that the information obtained from AIS in this situation can be cross-checked against other systems, the interviewees explained that this situation would not cause damage to the vessel nor nearby vessels. However, vessel spoofing does not have to result in disaster to be successful. An interviewee explained that if vessel spoofing were to happen during heavy fog in an area with dense traffic, they would reduce the speed of the vessel to get a better overview. This can result in financial loss if the vessel fails to meet the delivery time. Delayed goods can also affect other industries in terms of financial loss.

The interviewees agreed that SART spoofing could not be overlooked. However, the deck officers found it unlikely that this type of attack could lead to dangerous situations. It is reasonable to believe that a well crafted AIS attack can cause dangerous situations under the right circumstances. In a situation where the radar has reduced functionality due to heavy rain and rough sea, an attacker could perform a SART spoofing attack in combination with vessel spoofing. To nearby vessels, this could seem like a vessel in distress with a person overboard. The combination of a spoofed vessel and SART message could make the situation more trustworthy for nearby vessels.

As described in chapter 7, attacks on AIS in an AIS covered VTS area outside the radar coverage will reduce the safety in this area. When sailing in bad weather conditions with reduced vision, contradictory information received from an authority can create confusion and dangerous situations. From the interviews, it is not clear to what degree deck officers and maritime pilots trust information received from a VTS, especially contradictory information. However, considering that a VTS is a national authority, it is reasonable to assume that information obtained from a VTS

is regarded as trustworthy.

In general, there have been few malicious attacks targeting the maritime industry to disaster to this day. It is thus reasonable to believe this affects the somewhat carefree attitude towards the potential outcome of attacks.

8.5 Which cyber threat agent groups pose the highest threat against the industry?

RQ5: Based on the estimated cost and the potential outcomes of such attacks, which cyber threat agent groups pose the highest threat to the industry?

Only the six cyber threat agent groups that were addressed in section 2.3 will be considered in this section. Based on the groups' motivation and their capabilities, the two groups, Nation states and Insiders, have been considered to be the groups that pose the highest threat to the maritime industry.

Nation states have the past few years been accused of executing GNSS spoofing attacks on several occasions, as discussed in section 2.3. The threat agent group has political or military-based motivations that are achievable by launching such attacks. Furthermore, the group can launch such attacks with ease.

C4ADS identified in their report, as discussed in section 2.3 that the GNSS spoofing incidents that occurred were mainly due to the Russian Federation trying to protect the property of VIPs [C4A19]. Thus, the 1311 civilian vessels affected by the GNSS events were likely, in most cases, not affected to a high degree. Since the vessels most likely were not targeted by the Nation state, identifying that the GNSS receiver was not operating normally should, as a result, be a simple task by the navigator, as sudden positional jumps likely occurred during the GNSS events.

However, the incidents that have occurred during the past few years show the willingness Nation states have to use such techniques to obtain their goals. Even though C4ADS concluded that the GNSS spoofing techniques initiated by the Russian Federation were used as a protection mechanism, it shows the nation capabilities and willingness to use these techniques. Furthermore, few adjustments would be necessary to initiate a targeted attack towards a specific vessel, which could lead to fatal outcomes. Consequently, Nation states should be considered one of the groups which pose the highest threat to the maritime industry.

Insiders was the second most active cyber threat agent group during 2018, according to ENISA [SDM+19]. The group consists of agents that either have malicious intent or simply of agents that are naive or careless and thus make errors. The naive and careless agents that this group consists of are the reason why this

group is considered to pose a high threat to the maritime industry. Most AIS- and GNSS-based attacks aim to lure victims into acting in a manner that is favorable to the adversary. However, if the victim is observant and are aware of potential weaknesses within AIS and GNSS, the effectiveness of AIS- and GNSS-based attack may be limited. Yet, the overall awareness among navigators within the industry regarding potential AIS and GNSS attacks seemed to be somewhat limited based on the interviews that were held. Consequently, observant navigators must regularly cross-check information obtain from AIS and GNSS with alternative sources to ensure safe and correct navigation.

The following paragraphs argue why Cybercriminals, Hacktivists, Cyber terrorists, Script kiddies have been considered to pose a lower threat than Nation states and Insiders.

Cybercriminals were the most active group during 2018. This group is responsible for over 80% of the incidents, are mainly motivated by financial incentives [SDM+19]. However, AIS- and GNSS-based attacks aim in most cases to be disruptive and destructive, and to achieve this, the attacks often need to go unnoticed by the victim. Consequently, it is unclear how money should and could be extracted from the victims by launching such attacks without revealing that an attack is ongoing. Nevertheless, Cybercrime-as-a Service platforms have become an increasing trend, according to ENISA [SDM+19]. The increasing trend gives cybercriminals an incentive to execute such attacks. However, buyers are necessary, and the market for such attacks is likely pretty slim, mainly because the resources necessary to launch such attacks are substantial. As a consequence, cybercriminals do not pose a particularly high threat to the maritime industry concerning AIS and GNSS attacks. Despite this, the threat should not be neglected and should still be considered a real one.

Hacktivists are driven by political or geopolitical decisions and execute attacks as a way to draw media attention to push their cause. At the time of writing, several incidents affecting vessels within the maritime industry have occurred [C4A19]. Despite this, only a limited amount of news articles have been published. Thus, to achieve wide media coverage, a successful attack that leads to a severe outcome would likely be necessary. As a consequence, it is unlikely that AIS- and GNSS-based attacks would be conducted as alternative strategies would contribute more to their cause and be less costly.

Cyber Terrorists typically want to be credited to the attacks they execute. Additionally, the group is considered to have limited capabilities, according to ENISA [SDM+19]. Thus, stealthy GNSS and AIS attacks are less likely to be conducted, as it is hard to prove the origin of the attacks. Furthermore, other alternatives, such as

hijacking the vessels or inflict physical damage on the vessels, would be more likely events, as fewer resources and capabilities are required. However, the group should not be disregarded entirely as GNSS and AIS attacks still could be used to cause disastrous events which could be used to push their agenda.

Script Kiddies are the least active group and only have a limited set of capabilities. Nevertheless, only a limited set of resources is necessary to execute AIS- and GNSS-based attacks in a test environment. However, when executed on sailing vessels, additional equipment and knowledge are required. Thus, the threshold increases significantly when the attacks are executed on real targets. Despite this, it is not unthinkable that script kiddies could execute such attacks. However, alternative attacks that require fewer resources are more likely to be executed as they are easier to conduct.

8.6 Countermeasures

RQ6: Which techniques could be implemented to thwart the attacks?

GNSS and AIS are two widely used technologies within the maritime industry. However, both of the technologies possess severe vulnerabilities, which makes it complicated to determine whether the signals obtained are authentic. Researchers have, as a result, published a wide range of papers where potential solutions are proposed.

Psiaki et al. stated in their paper that cryptography, direction-of-arrival sensing, and signal-distortion detection are the three main classes available to thwart spoofing attacks [PH16a].

Cryptographic schemes require modifications both at the receiving and the transmitting side and is somewhat a weakness of this class. The cost of implementing such a scheme is substantial as the cryptographic scheme needs to be determined, tested, and implemented both at the transmitting and receiving side. Additionally, cryptographic schemes will cause additional overhead on the GNSS bandwidth, which is already a scarce resource and needs to be taken into consideration when determining a scheme. Nevertheless, GSA has announced that within 2020 a commercial service will be available where encryption can be activated [Age17]. It is important to note that some cryptographic schemes may thwart the possibility to generate and transmit seemingly legitimate GNSS signals at will. However, if no mechanism is set in place to ensure the freshness of the signals, retransmitting of previous recorded GNSS signals can be executed and is another possible method to launch a spoofing attack.

The direction-of-arrival sensing and signal-distortion detection class have similar strengths and weaknesses. The detection techniques are only implemented on the

receiving device, which makes it possible for individual companies to develop and construct detection techniques based on their desire, as no standardization is necessary. This is consequently a strength, as several types of techniques are constructed, which make it possible by the end-user to choose the product that is thought to be the most effective. Additionally, fewer resources are necessary to implement such techniques compared to the amount required to implement a cryptographic based scheme. However, a substantial cost will still be required from the manufacturers as additional hardware and research are necessary. Furthermore, direction-of-arrival sensing and signal-distortion detection are primarily used for detection purposes rather than a mechanism to thwart spoofing attacks completely. Hence, spoofing attacks will still be possible in many cases, but the users will be aware that the received signals could be malicious.

AIS is not as widely used as GNSS, which is why less research has been conducted in the field. Nevertheless, several strategies have been proposed to help mitigate the current vulnerabilities existing in the system. Every identified method in section 2.2.3 falls under the same category, namely cryptographic-based techniques. As already mentioned, to create effective cryptographic-based techniques, standardization is necessary and requires a lot of effort and resources. However, AIS and GNSSs fundamentally differ in the sense that AIS transceivers both transmit and receive signals, which is not the case for GNSS receivers. The difference adds extra complexity that needs to be addressed when implementing a cryptographic-based scheme in AIS-based systems.

Furthermore, the transition from AIS transceivers transmitting messages in the clear to transceivers transmitting messages based on a cryptographic scheme has several obstacles that need to be handled appropriately. One of the primary obstacles is how transceivers without cryptographic capabilities should communicate with transceivers with cryptographic capabilities. Thus, questions such as, should transceivers with cryptographic capabilities accept messages that are not protected, and how should transceivers with no cryptographic capabilities get a situational overview, if the messages are encrypted or are on an unknown format arise and needs to be answered. AIS was developed to increase the navigational and situational awareness. However, if the transition is not handled correctly, the transitional period between having transceivers with no cryptographic capabilities to having a vast majority of transceivers with cryptographic capabilities could result in a time frame where the value of the AIS would be massively reduced.

Due to the nature of how AIS operates and the architecture of the system, additional techniques based on direction-of-arrival sensing and signal-distortion detection are not viable.

Increasing the awareness of the operators using navigational equipment is an alternative method that has been discussed and could, as a result, decrease the severity of the attack. The method would likely be less costly than the technical solutions. However, detection of a potential attack may, in some cases, be infeasible as not all information can be verified by other systems or methods. Thus, additional training to understand the weaknesses of the systems only help to a certain extent.

The reason that few measures have been developed to improve the overall security within AIS- and GNSS-based systems is a debatable question. The systems were designed without security in mind. As a result, dozens of strategies have been proposed to solve the vulnerabilities. However, several decades later, few measures have been implemented. The lack of change is likely a result of few incidents resulting in severe outcomes, relatively low pressure from the community, and that it may not be considered cost-efficient.

8.7 Validity of results

Neither the GPS-based attacks nor the AIS-based attacks were initiated on navigational equipment that are used within the maritime industry, as such equipment was not obtainable. Despite this, as the signals forged by attacks were received and accepted as legitimate signals by the receiving devices, maritime equipment with no detection techniques are assumed to accept the signals similarly as the equipment used in the experiments.

The resource cost estimates are mainly based on online prices. Costs such as tax and expenses related to transporting necessary equipment have not been considered. Additionally, the equipment and services that are sold online are subject to change, which may consequently make the estimates less accurate.

Only a small group of eight participants with different experiences and roles in the maritime industry were interviewed during this master thesis. It is, therefore, important to note that their opinion and knowledge do not necessarily represent the maritime industry as a whole. Thus, to generalize large parts of the maritime industry and discuss how they handle cybersecurity incidents solely based on the interviews may be misleading or incorrect. It is therefore important to note that when cybersecurity within the maritime industry is discussed, it is with a focus on the three groups that were interviewed.

8.8 Ethics

This master thesis explains in great detail how to execute a wide range of AIS- and GNSS-based attacks. Necessary equipment, dependencies, modifications of the respective software, and steps necessary to build and execute the attack are all well explained. Thus, replication of the attacks become a simple task if the same procedure is followed. Furthermore, several interviews were held with participants operating AIS- and GNSS-based systems daily. Based on the interviews, it became clear that the interviewees were not aware of the underlying vulnerabilities within the systems and consequently were not aware of the extent of the types of attacks that are possible. Consequently, the results obtained in the master thesis can be exploited by malicious agents, as the thesis further decreases the complexity of AIS- and GNSS-based attacks and identifies the lack of awareness within at least a part of the industry. However, to make cybersecurity a top priority within the maritime industry, weaknesses, and risks need to be identified as it will push the industry in the right direction.

Chapter 9
Conclusion and Future Work

The global shipping industry transport an estimated 90% of all world trade and has an essential role in the global economy [TJ18]. Modern vessels are increasingly becoming more dependent on digital systems to efficiently and safely navigate. With autonomous vessels on the horizon, this trend is not likely to stop anytime soon. Nevertheless, widely known vulnerabilities within two core navigational systems, the AIS and the GNSS, are still present. As a consequence, a wide range of attacks are possible. These attacks have become more feasible with time, as necessary hardware components have become more affordable and as open-source software has become accessible. Thus, previously non-threat agents with limited capabilities have become potential threats.

Although the attacks are becoming less complicated, the threat landscape seems still to be mostly dominated by Nation states and Insiders [GPS17] [WB19] [C4A19]. However, few AIS and GNSS related incidents have resulted in severe outcomes. It is reasonable to assume that this affects the lack of adequate measures that have been taken to mitigate the vulnerabilities.

Three marine pilots, four deck officers, and a maritime traffic leader were interviewed during the master thesis. Each of the interviewees uses AIS and GNSS services daily. However, the overall awareness of potential attacks affecting AIS and GNSS is considered low. The interviewees were only familiar with a few of the attacks affecting the systems. Despite using the systems regularly, out of all the interviewees, only the maritime traffic leader considered the systems as a necessity to conduct the tasks safely. In other words, neither the marine pilots nor the deck officers considered AIS- and GNSS-based attacks to be an issue affecting the safety of the vessels, as they did not rely on the systems to a high degree, to begin with.

Previously presented findings from relevant literature states that deck officers, in general, trust the positional data obtained from GNSSs to a high degree. Additionally, their attention is largely directed towards the Electronic Chart Display and

Information System (ECDIS) [HOM16]. However, from the interviews, the marine pilots and deck officers mistrust most of the discussed electronic systems, except radar. AIS was especially considered unreliable as the data obtained by the AIS transceivers have, on several occasions, been inaccurate or incorrect. Nevertheless, as the interviewees do not represent every marine pilot and deck officer operating in Norwegian waters, a conclusion cannot be drawn.

Future Work

For future work, commercial maritime AIS and GNSS equipment should be tested to verify that the equipment responds to the attacks as expected. This is especially important in the case of the AIS-based attacks, where some attacks conducted in chapter 5 did not get the anticipated response from the equipment at hand. The equipment and software used in the AIS experiment might not have the same functionality as a commercial AIS, which could be the reason the equipment responded unexpectedly.

Furthermore, interviews containing more than eight participants should be held to investigate whether the knowledge and the opinions that were discovered are widespread throughout the industry. Alternatively, a survey could be utilized to answer this question and would make it easier to include more participants.

Practical experiments where pilots and deck officers experience AIS- and GNSS-based attacks would make it possible to identify how they respond in case of such events. It would be important to provide the pilots and deck officers with limited information regarding the experiment, to make the experience as authentic as possible. However, a considerable amount of resources would be necessary to conduct such an experiment in open waters. Additionally, it would be important that the experiment did not interfere with vessels outside of the experiment.

Only a subset of the resource alternatives identified in chapter 6 has been assigned a cost estimate. Thus for future work, all the resource alternatives identified should get an associated cost range. By giving all the resource alternatives an associated cost range, a complete picture will be obtainable, which will make it easier to prepare for potential attacks.

As we are moving closer to an era of fully autonomous vessels, electronic navigation systems will play a key role in how the vessels operate. As a consequence, the importance of robust and secure navigational systems will be more vital than ever. Essential services offered by AIS and GNSS are more vulnerable as no deck officers will be present and able to monitor and cross-check information received by the navigation systems. Consequently, how companies that are currently developing autonomous vessels are trying to overcome these obstacles should be investigated

in future work. Additionally, future research should investigate whether AIS- and GNSS-based attacks will be effective on autonomous vessels.

References

[Adma] The Norwegian Coastal Administration. About the PEC agreement. https://www.kystverket.no/en/EN_Maritime-Services/Pilot-Exemption-Certificate/Pilot-Exemption-Certificate-/.

[Admb] The Norwegian Coastal Administration. Vessel Traffic Service. https://www.kystverket.no/en/EN_Maritime-Services/Vessel-Traffic-Service/.

[Adm11a] The Norwegian Coastal Administration. Compulsory pilotage. https://www.kystverket.no/en/EN_Maritime-Services/Pilot-Services/Compulsory-pilotage/, 08 2011.

[Adm11b] The Norwegian Coastal Administration. SafeSeaNet Norway. https://www.kystverket.no/en/EN_Maritime-Services/Reporting-and-Information-Services/SafeSeaNet-Norway/, 08 2011.

[Adm11c] The Norwegian Coastal Administration. Vessel Traffic Service (VTS). https://www.kystverket.no/en/EN_Maritime-Services/Vessel-Traffic-Service/VTS-Services/, 08 2011.

[Age] European Space Agency. Satellite - Automatic Identification System (SAT-AIS) Overview. https://artes.esa.int/sat-ais/overview.

[Age11] European Space Agency. GPS General Introduction - Navipedia. https://gssc.esa.int/navipedia/index.php/GPS_General_Introduction, 2011.

[Age17] European GNSS Agency. Galileo Commercial Service Implementing Decision enters into force. https://www.gsa.europa.eu/sites/default/files/content/press_releases/pr-gsa-09-03_2017_galileo_commercial_service_implementing_act.pdf, 02 2017.

[AIS] All About AIS. Frequency. http://www.allaboutais.com/index.php/en/technical-info/technical-fundamentals/109-ais-technicals/various-ais-technologies/158-frequency.

[Ako12] Dennis M Akos. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *NAVIGATION: Journal of the Institute of Navigation*, 59(4):281–290, 2012.

[And16] Andrmarkv. Problem simulating when using USRP B200 · Issue #50 · osqzss/gps-sdr-sim. https://github.com/osqzss/gps-sdr-sim/issues/50, 10 2016.

[Art13] Charles Arthur. Thousands using GPS jammers on UK roads pose risks, say experts. https://www.theguardian.com/technology/2013/feb/13/gps-jammers-uk-roads-risks, 02 2013.

[Ass16] International Maritime Pilots' Association. Guidelines On The Design And Use Of Portable Pilot Units International Maritime Pilots' Association With Technical Input From Comité International Radio-Maritime (CIRM). http://www.impahq.org/admin/resources/guidelines.pdf, 2016.

[Bar13] Barentswatch. AIS displays status report at sea. https://www.barentswatch.no/en/articles/AIS-displays-status-report-at-sea/, 05 2013.

[BJJD+12] Ali Broumandan, Ali Jafarnia-Jahromi, Vahid Dehghanian, John Nielsen, and Gérard Lachapelle. GNSS spoofing detection in handheld receivers based on signal spatial correlation. In *Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium*, pages 479–487. IEEE, 2012.

[BMTK15] Joanna Brooks, Serena McCluskey, Emma Turley, and Nigel King. The utility of template analysis in qualitative psychology research. *Qualitative research in psychology*, 12(2):202–222, 2015.

[BPW14] Marco Balduzzi, Alessandro Pasta, and Kyle Wilhoit. A security evaluation of AIS. In *Proceedings of the 30th annual computer security applications conference*. ACM, 2014.

[BYK18] Simon Lau Boung Yew and Keh Kim Kee. Artificial Neural Network Back-Propagation Based Decision Support System for Ship Fuel Consumption Prediction. page 1, January 2018.

[C4A19] C4ADS. Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria. https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf, 2019.

[CCGF16] Nicholas Clifford, Meghan Cope, Thomas Gillespie, and Shaun French. *Key methods in geography*, page 147. Sage, 2016.

[CCSL17] Gianluca Caparra, Silvia Ceccato, Silvia Sturaro, and Nicola Laurenti. A key management architecture for GNSS open service Navigation Message Authentication. In *2017 European Navigation Conference (ENC)*, pages 287–297. IEEE, 2017.

[CDQ+19] A.W. Coburn, J. Daffron, K. Quantrill, E. Leverett, J. Bordeau, A. Smith, and T. Harvey. Cyber risk outlook. page 25, May 2019.

[Cre13] GPS Creations. Price List -Effective. http://www.gpscreations.com/NewFiles/Price%20List.pdf, 2013.

[Deb] Debian. socat. https://manpages.debian.org/testing/socat/socat.1.en.html.

[Del] Delock. Delock Products 88451 Delock LTE Antenna SMA plug 1 - 4 dBi omnidirectional with tilt joint black. https://www.delock.de/produkte/G_88451/merkmale.html?setLanguage=en.

[Ebi20] Takuji Ebinuma. osqzss/gps-sdr-sim. https://github.com/osqzss/gps-sdr-sim, 02 2020.

[Fos] Nick Foster. bistromath/gr-ais. https://github.com/bistromath/gr-ais.

[ge11] ggsc esa. BeiDou General Introduction - Navipedia. https://gssc.esa.int/navipedia/index.php/BeiDou_General_Introduction, 2011.

[GHC+13] Nicola K Gale, Gemma Heath, Elaine Cameron, Sabina Rashid, and Sabi Redwood. Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC medical research methodology*, 13(1):2, 2013.

[GK19] Athanassios Goudossis and Sokratis K Katsikas. Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology*, 24(2):411, 2019.

[GLO] GLONASS. Glonass history. https://www.glonass-iac.ru/en/guide/.

[Gnu20] GnuRadio. UbuntuInstall - GNU Radio. https://wiki.gnuradio.org/index.php/UbuntuInstall, 02 2020.

[go] gr osmosdr. gr-osmosdr - GNU Radio block for interfacing with various radio hardware. https://git.osmocom.org/gr-osmosdr/about/.

[GOVa] GPS GOV. Gps.gov: New civil signals. https://www.gps.gov/systems/gps/modernization/civilsignals/?fbclid=IwAR1gCfplBuzBtWyQlYvmtU5GqNQ-KtXIg3ucleaE1BVjqqd3VpKl1GbcLrM.

[GOVb] GPS GOV. Other Global Navigation Satellite Systems (GNSS). https://www.gps.gov/systems/gnss/.

[GPS95] GPS. Global Positioning System Standard Positioning Service Signal Specification 2nd edition. page 9, 1995.

[GPS17] GPSworld. Spoofing in the Black Sea: What really happened? https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/, 10 2017.

[Hag19] Kristian Haga. Resource Cost Estimate Model | TDT4501 - Computer Science, Specialization Project, 2019.

[HCA11] Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1(1), 2011.

[HLB+15] John Hall, Jordan Lee, Joseph Benin, Christopher Armstrong, and Henry Owen. IEEE 1609 influenced automatic identification system (AIS). In *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, pages 1–5. IEEE, 2015.

[HLP+08] Todd E Humphreys, Brent M Ledvina, Mark L Psiaki, Brady W O'Hanlon, and Paul M Kintner. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Radionavigation laboratory conference proceedings*, 2008.

[HOM16] Odd Sveinung Hareide, Runar Ostnes, and Frode Voll Mjelde. Understanding the Eye of the Navigator. page 1, 2016.

[IMOa] IMO. International Convention for the Safety of Life at Sea (SOLAS), 1974. http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx.

[IMOb] IMO. International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978. http://www.imo.org/en/OurWork/HumanElement/TrainingCertification/Pages/STCW-Convention.aspx.

[INR+16] Clément Iphar, Aldo Napoli, Cyril Ray, Erwan Alincourt, and David Brosset. Risk Analysis of falsified Automatic Identification System for the improvement of maritime traffic safety. December 2016.

[IR14] ITU-R. Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band. https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1371-5-201402-I!!PDF-E.pdf, 02 2014.

[Jam] Perfect Jammer. Super Large Range 1500-2000 Meters Long Distance Jamming. https://www.perfectjammer.com/1500-2000-meters.html.

[Jef10] Charles Jeffrey. *An Introduction to GNSS GPS, GLONASS, Galileo and other Global Navigation Satellite Systems*, pages 6–12. 2010.

[Kin18] Alex King. Seven things you should know about AIS. https://www.marinetraffic.com/blog/seven-things-know-ais/, 01 2018.

[Lab] LabSat. Free GPS NMEA Simulator software. https://www.labsat.co.uk/index.php/en/free-gps-nmea-simulator-software.

[Lab17] Silicon Labs. RF Range Calculator. https://www.silabs.com/community/wireless/proprietary/knowledge-base.entry.html/2017/05/02/rf_range_calculator-SYIA, 05 2017.

[Man86] Samir Mankabady. *The International Maritime Organization, volume 1: International Shipping Rules.* 1986.

[Mar] MarineTraffic. MarineTraffic Online Services | MarineTraffic. https://www.marinetraffic.com/en/online-services/single-services/sat-global.

[Meh15] Mehdi. Problem with running · Issue #26 · osqzss/gps-sdr-sim. https://github.com/osqzss/gps-sdr-sim/issues/26, 12 2015.

[Mic17] Trend Micro. encode21 not in source · Issue #4 · trendmicro/ais. https://github.com/trendmicro/ais/issues/4, 11 2017.

[Mor90] Janice M Morse. *Qualitative nursing research: A contemporary dialogue*, pages 127–145. Sage Publications, 1990.

[NAS12] NASA. Global Positioning System History. https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html, 10 2012.

[NAS20] NASA. Broadcast ephemeris data. https://cddis.nasa.gov/Data_and_Derived_Products/GNSS/broadcast_ephemeris_data.html#:~:text=The%20daily%20GPS%20broadcast%20ephemeris, 2020.

[No16] IALA Guideline No. 1082 An Overview of AIS. *International Association of Marine Aids to Navigation and Lighthouse (June 2016)*, June 2016.

[Nov15] Novatel. Unintentional Interference. https://www.novatel.com/tech-talk/velocity/velocity-2015/unintentional-interference/, 2015.

[Ope] OpenCPN. About OpenCPN. https://opencpn.org/OpenCPN/info/about.html.

[Oss17] Michael Ossmann. mossmann/hackrf. https://github.com/mossmann/hackrf/wiki/HackRF-One, 09 2017.

[Par14] M. W. Parsons. Encrypted Automatic Identification System (EAIS) Interface Design Description (IDD), 2014.

[PH16a] Mark L Psiaki and Todd E Humphreys. GNSS spoofing and detection. *Proceedings of the IEEE*, 104(6):1258–1270, 2016.

[PH16b] Mark L Psiaki and Todd E Humphreys. Protecting GPS From Spoofers Is Critical to the Future of Navigation, 07 2016.

[Pol10] Denise F Polit. *Essentials of nursing research*, pages 295–341. Wolters Kluwer Health/Lippincott Williams & Wilkins, 2010.

[Pul] Pulselarsenantennas. PulseLarsen Antennas | W1900. https://www.pulselarsenantennas.com/product/w1900/.

[rad19a] GNU radio. Handling Flowgraphs - GNU Radio. https://wiki.gnuradio.org/index.php/Handling_Flowgraphs, 2019.

[rad19b] GNU radio. What is GNU Radio? - GNU Radio. https://wiki.gnuradio.org/index.php/What_is_GNU_Radio%3F, 2019.

[Resa] Ettus Research. B200/B210/B200mini/B205mini - Ettus Knowledge Base. https://kb.ettus.com/B200/B210/B200mini/B205mini.

[Resb] Ettus Research. files.ettus.com:/binaries/images/. https://files.ettus.com/binaries/images/.

[Res13] Ettus Research. USRP Hardware Driver and USRP Manual: Binary Installation. https://files.ettus.com/manual/page_install.html, 08 2013.

[Res19] Ettus Research. EttusResearch/UHD. https://github.com/EttusResearch/uhd/tree/master/host/, 2019.

[Res20] Ettus Research. EttusResearch/UHD. https://github.com/EttusResearch/uhd, 04 2020.

[Sch99] Bruce Schneier. Attack trees. *Dr. Dobb's journal*, 24(12):21–29, 1999.

[SDM+19] Andreas Sfakianakis, Christos Douligeris, Louis Marino, Marco Lourenço, and Omid Raghim. ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends, 01 2019.

[SM] Susanne Stephansen and Tor Midtbø. The Norwegian National Coastal Administration. https://www.regjeringen.no/en/dep/sd/organisation/subordinate-agencies-and-enterprises/the-norwegian-national-coastal-administr/id115310/.

[SM19] Susanne Stephansen and Tor Midtbø. Norwegian Coastal Administration (NCA). https://www.regjeringen.no/en/dep/sd/english-content/norwegian-coastal-administration-nca/id2343456/, May 2019.

[SOL] SOLAS. Solas Chapter V - Regulation 19 - Carriage requirements for shipborne navigational systems and equipment. http://solasv.mcga.gov.uk/regulations/regulation19.htm, urldate = 2020-05-06.

[Tho00] Sally Thorne. Data analysis in qualitative research. *Evidence-based nursing*, 3(3):68–70, 2000.

[TJ18] Kimberly Tam and Kevin Jones. Cyber-risk assessment for autonomous ships. In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, page 1. IEEE, 2018.

[TJ19] Kimberly Tam and Kevin Jones. MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18(1):129–163, January 2019.

[WB19] Michelle Wiese Bockmann. Seized UK tanker likely 'spoofed' by Iran. https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran, 08 2019.

[Wes06] Andreas Westerberg. A cost benefit analysis of the ais [automatic identification system] system in sweden. Master's thesis, 2006.

[Whi08] Lisa S. Whiting. Semi-structured interviews: guidance for novice researchers. *Nursing Standard (through 2013)*, 22(23):35–40, Feb 2008. Copyright - Copyright RCN Publishing Company Feb 13-Feb 19, 2008; Last updated - 2016-04-30; CODEN - NSTAEU.

Appendix A
Interview Guide

Interview Guide

Goal of the interviews:

The main goals of the interviews are to get a better understanding on how important AIS and GNSS are to be able to navigate precisely, what kind of backup routines and systems are available in case of a failure, and the overall awareness users of AIS/GNSS have regarding the underlying cybersecurity risks when using the system.

Introduction:

- What is the interviewee's occupation, and can the interviewee tell a bit about how a typical day goes?
- For how long has the interviewee been in that position?
- **Maritime pilot** specific questions:
  - Number of vessels operated daily?
  - How large are typical the vessels operated?
  - Is the equipment typical standardized/similar from vessel to vessel?
    - Or is a Portable Pilot Unit (PPU) used for navigation?
- **Captain and Chief Mate** specific questions:
  - How large is the vessel the interviewee is operating?
  - Which year was the vessel built?
- **Maritime traffic leader** specific questions:
  - What is the services the Norwegian Vessel Traffic Service (VTS) offers?

    - Starting points:
        - Information Service (INS)
        - Navigation Assistance Service (NAS)
        - Traffic Organisation (TOS)

- What kind of equipment does the interviewee use for navigation purposes?
- To what degree are processes/systems used for navigation autonomous?

Main:

- **AIS/GNSS dependency**
    - What is the interviewee's experience with AIS/GNSS?
    - For what purpose does the interviewee use AIS/GNSS?
    - How critical are AIS and GNSS?
    - How important are the systems for precise navigation?
        - And what is considered as precise navigation in narrow waters (How many meters uncertainty)?
    - How does the interviewee ensure that the vessel stays at the correct route?
    - What is purpose behind using AIS/GNSS within the organisation?
        - How vital is AIS for the organisation?
        - To what degree does the importance increase/decrease under conditions such as:
            - Day vs night
            - Clear sight vs fog
    - At what particular point does the interviewee considered AIS as most valuable?

- **In case of an incident**
  - What systems are available in the case of AIS/GNSS failure?
  - Have the interviewee experienced inaccurate data to a degree where backup systems were necessary to navigate accurately?
  - Is the interviewee (or the staff in general) aware of the potential threats to AIS/GNSS?
    - Starting points:
      - If the interviewee is familiar with threats to AIS/GNSS, Where did the interviewee learn about the vulnerabilities in AIS/GNSS?
      - AIS/GNSS spoofing attacks?
      - AIS/GNSS jamming attacks?
      - AIS Sart Spoofing
  - Is the staff regularly trained to navigate without AIS/GNSS?
  - What would be the worst-case if such an event took place?
  - Is a report constructed in case of an incident that affects systems such as those who are based on AIS/GNSS?
    - If this is the case, who obtains the report?
- **Protection mechanisms**
  - Is the interviewee aware of if any specialized equipment or methods that are used to thwart attacks on AIS/GNSS?
    - If so, can the interviewee elaborate regarding what is used?

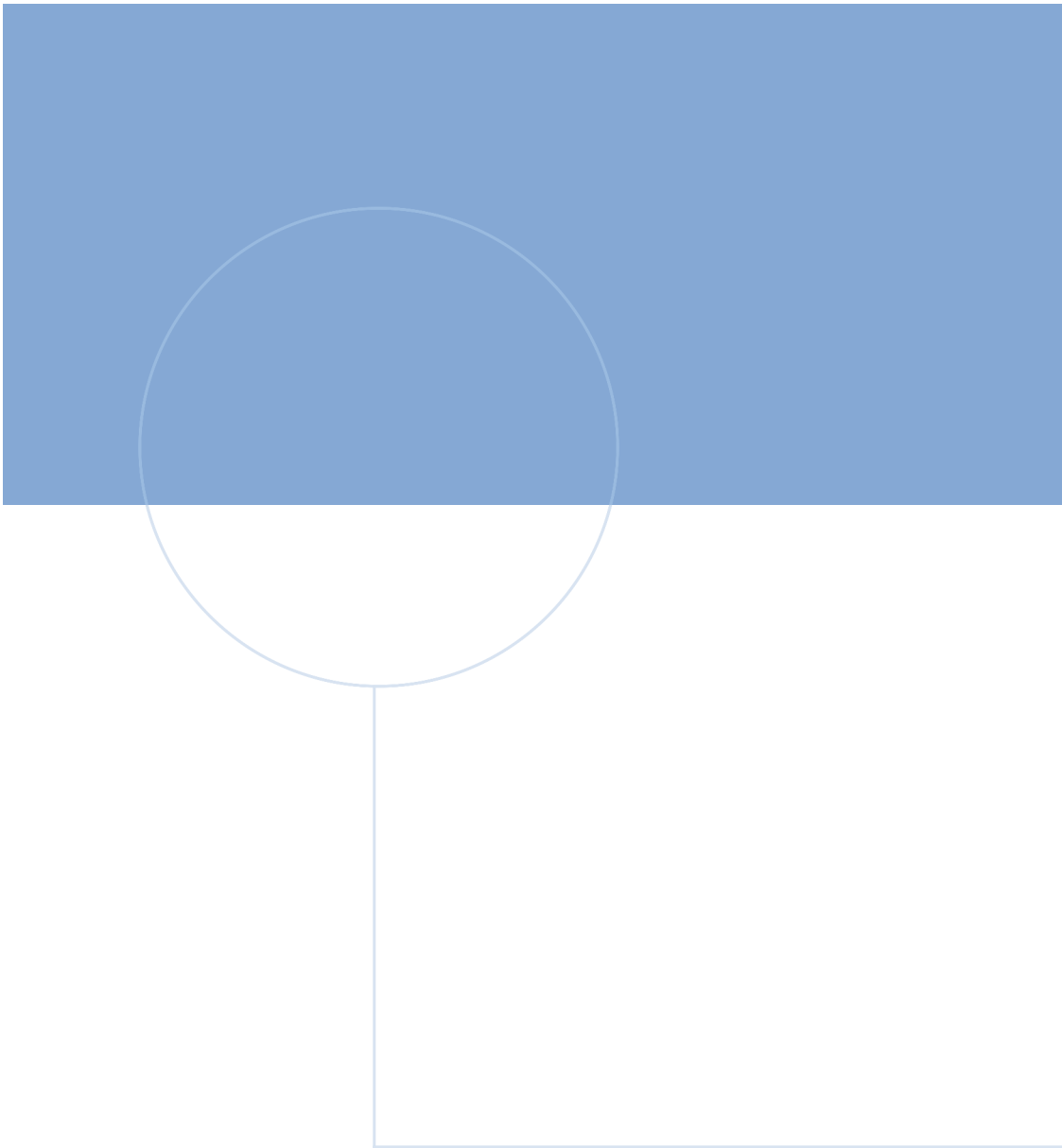
Round off questions:

- Is there anything the interviewee wants to add?
- Information about the project going forward

Appendix B
AIS message types

Type	Name	Description
1	Position report	Class A, scheduled positional report
2	Position report	Class A, assigned scheduled positional report
3	Position report	Class A, positional report (response to interrogation)
4	Base station report	Positional and time reference report
5	Static and voyage related data	Class A, ETA, destination and similar data (updated manually)
6	Binary addressed message	Point-to-point message (unspecified payload)
7	Binary acknowledgement	Acknowledgement of received type 6 data
8	Binary broadcast message	Broadcast messages (binary)
9	Standard SAR aircraft Position report	Tracking data for SAR aircrafts
10	UTC/Date inquiry	Request UTC/Date information
11	UTC/Date response	Response to UTC/Date request
12	Addressed safety related message	Point-to-point text message
13	Safety-Related Acknowledgemente	Acknowledgement of received message of type 12
14	Safety-Related Broadcast Message	Broadcast text message

Type	Name	Description
15	Interrogation	Query AIS transponder for status
16	Assignment mode command	Configure scheduling of AIS information messages (control authority)
17	DGNSS broadcast binary message	DGNSS corrections
18	Standard Class B equipment position report	Class B, Positional report
19	Extended Class B equipment position report	Class B, Extended positional report
20	Data link management message	Reserve time slot for base station
21	Aids-to-Navigation report	Status and location for aids to navigation (AtoN)
22	Channel management	Set VHF parameters (control authority)
23	Group Assignment Command	Set operational parameters for mobile stations in a specified area
24	Static Data Report	Class B, ETA, destination and similar data (updated manually)
25	Single slot binary message	Unscheduled binary data
26	Multiple slot binary message with Communications State	Scheduled binary data
27	Position report for long range applications	Class A, scheduled position report (outside base station coverage)



NTNU

Norwegian University of
Science and Technology