IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 21, 2021, accepted February 23, 2022, date of publication March 11, 2022, date of current version March 21, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3158943

Cybersecurity Attacks on Software Logic and Error Handling Within AIS Implementations: A Systematic Testing of Resilience

SYED KHANDKER, HANNU TURTIAINEN, ANDREI COSTIN, AND TIMO HÄMÄLÄINEN
Faculty of Information Technology, University of Jyväskylä, 40014 Jyväskylä, Finland

Corresponding author: Andrei Costin (ancostin@jyu.fi)

This work was supported in part by the Finnish Grid and Cloud Infrastructure (FGCI) (persistent identifier urn:nbn:fi:research-infras-2016072533), in part by the Decision of the Research Dean on Research Funding within the Faculty of Information Technology of the University of Jyväskylä, and in part by the Finnish Cultural Foundation under Grant Decision 00211119.

ABSTRACT To increase situational awareness of maritime vessels and other entities and to enable their exchange of various information, the International Maritime Organization mandated the use of the Automatic Identification System (AIS) in 2004. The AIS is a self-reporting system that uses the VHF radio link. However, any radio-based self-reporting system is prone to forgery, especially in situations where authentication of the message is not designed into the architecture. As AIS was designed in the 1990s when cyberattacks were in their infancy, it does not implement authentication or encryption; thus, it can be seen as fundamentally vulnerable against cyberattacks. This paper demonstrates and evaluates the impact of multiple cyberattacks on AIS via remote radio frequency (RF) links using transmission-enabled software-defined radio (SDR). Overall, we implemented and tested a total of 11 different tests/attacks on 19 AIS setups, using a controlled environment. The tested configurations were derived from heterogeneous platforms such as Windows, Android, generic receivers, and commercial transponders. Our aim is to enhance the early discovery of new vulnerabilities in AIS to effectively address AIS attacks in the nearest future. The results showed that approximately 89% of the setups were affected by Denial-of-Service (DoS) attacks at the AIS protocol level. Besides implementing some existing attack ideas (e.g., spoofing, DoS, and flooding), we showed some novel attack concepts in the AIS context such as a coordinated attack, overwhelming alerts, and logical vulnerabilities, all of which have the potential to cause software/system crashes in the worst-case scenarios. Moreover, an implementation/specification flaw related to the AIS preamble was identified during the experiments, which may affect the interoperability of different AIS devices. The error-handling system in AIS was also investigated. Unlike the aviation sector's Automatic Dependent Surveillance-Broadcast (ADS-B), the maritime sector's AIS does not effectively support any error correction method, which may contribute to RF pollution and less effective use of the overall system. The consistency of our results for a comprehensive range of hardware-software configurations indicated the reliability of our approach, test system, and evaluation results.

INDEX TERMS AIS, attacks, cybersecurity, DoS, maritime, resiliency, ship.

I. INTRODUCTION

TO facilitate the growing world trade, the number of commercial cargo carriers is increasing. Also, many other vessels share the same waterways, such as leisure boats, fishing boats, and passenger ships. To improve the safety of navigation and to avoid collisions, the International Maritime Organization (IMO) announced in 2004 the mandatory use of the Automatic Identification System [1]. AIS is an automatic tracking system that periodically transmits a ship's type, name, position, speed, and other data to nearby vessels and other maritime entities. It is a prevalent maritime situational awareness system used by approximately 570,000 vessels [2]. AIS uses a VHF radio link to transmit and receive signals. It is a self-reporting system wherein the trustworthiness of information depends on the data being reported by the vessel

The associate editor coordinating the review of this manuscript and approving it for publication was Tyson Brooks.

rather than measured by radar. However, any self-reporting system over a radio link is exposed to security vulnerabilities due to the possibility of spoofing. To prevent spoofing, security measures such as authentication or encryption are necessary. However, the current AIS protocol does not utilize any authentication or encryption methods; therefore, it is exposed to serious cybersecurity threats.

There have been several incidents of exploitation of the AIS system. On June 19, 2021, an online ship tracking site showed that a British warship and a Dutch frigate were close to Sevastopol in Crimea, which escalated tension between Russia and Britain. However, the on-board cameras of both ships revealed that they were roughly 300 km away [3]. In another case, North Korean vessels altered the Maritime Mobile Service Identity (MMSI) of their fishing ship to evade sanctions. Under their false identity, they were found fishing near the coastal area of China [4]. Finally, unknown entities were falsely claiming to be the US or coalition warships near the strait of Hormuz [5]. Such reports indicate that AIS has already been exploited at the national or military level. Such sensitive dangerous security flaws have not yet been thoroughly investigated in academia. Only a handful of studies practically investigated the such flaws [6]. In the meantime, malicious attacks on AIS threaten to spread at the ordinary hacker level due to the proliferation of low-cost, transmission-enabled software-defined radio (SDR) technology that has made it possible to produce any radio signal at a low cost and effort. For example, our laboratory had two types of transmission-enabled SDR, HackRF and BladeRF. Each of them, though costing less than $500, was able to produce fake AIS signals. Missing basic security measures and the evolution of transmission-enabled SDR technology have forced this three-decades-old AIS technology to face unprecedented challenges from cybersecurity attacks. Nonetheless, all vessels in the vast waterways have to follow the current AIS protocol, which is insecure by default.

AIS receivers are also diversifying day by day. Besides the traditional on-board AIS setup, smartphone-based navigation applications are also broadly used. The 7 smartphone-based navigation applications used in this study were downloaded approximately 43,000 times from the Google play store, leaving alone other non-tested applications and iOS platform's download numbers aside. The navigation data are fed to the mobile application from the receiver through a WiFi connection. These smartphone-based receiving setups, due to their attractive graphical user interface, low cost, and ease of installation, are gaining popularity among private users. However, these types of portable receivers remain untested against cyberattacks, as shown in current literature. Lack of extensive study of AIS exploitation, insufficient study on the impact of cyberattacks on modern AIS setups, and our previous security experience on a similar aviation service (Automatic Dependent Surveillance-Broadcast (ADS-B) [7], [8]) have motivated us to conduct this study. The main contributions of this study are:

1) Some novel (and existing) attacking concepts on AIS – such as spoofing, jamming, Denial-of-Service (DoS), coordinated attack, collision alert, overwhelming alerts, logically invalid data encoding, man overboard, etc., – were practically implemented and evaluated over the radio link;
2) Logic vulnerabilities, error handling and coordinated attacks in AIS were studied for the first time (to the best of our knowledge); and
3) An important AIS preamble-related implementation flaw was identified and investigated.

The rest of this article is organized as follows. Details of the AIS technology are described in Section II. Related studies are discussed in Section III. Details of our test platform, attack implementation, and experimental setup are presented in Section IV. Our attacks, results, and analysis are explained in Section V. Some countermeasures to attacks are discussed in Section VI. Finally, possible workarounds, future studies, and conclusions are presented in Section VII.

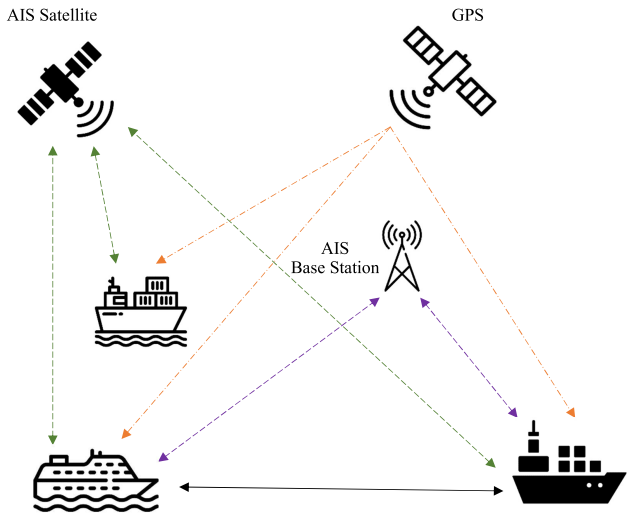


FIGURE 1. AIS communication architecture.

II. OVERVIEW OF AUTOMATIC IDENTIFICATION SYSTEM

The AIS is a worldwide automatic ship tracking system that based on fits into vessel as small transponders that periodically transmit the ship name, type, MMSI, speed, navigation status, and other useful information using the VHF radio signal. The most important information in the AIS data is the location information, which is generally obtained from the Global Navigation Satellite System (GNSS) such as the Global Positioning System (GPS). AIS uses two radio channels: channel A at 161.975 MHz (denoted as 87B) and channel B at 162.025 MHz (denoted as 88B). A dual-channel system is used to increase the link capacity and to minimize the RF interference. Using these two channels, ships can communicate with other ships, base stations, or other entities (e.g., stationary boys and men overboard). Due to the earth's

curvature and antenna height, the typical range of AIS signals is limited to approximately 40 nautical miles. If two ships cannot communicate directly, they can still exchange information via a base station or satellite called SAT-AIS. However, SAT-AIS is not yet fully operational across the globe. To date, countries such as USA, Canada, Norway, and India launched a few satellites to conduct full-scale research on SAT-AIS. Figure 1 shows the AIS communication concept. It enables different types of vessels to exchange information directly or via a base station or a satellite. There are mainly five types of AIS devices:

- Class A uses the Self-Organized Time Division Multiple Access (SOTDMA) scheme. Its nominal transmission power is 12.5 watts. It is mainly used by large commercial vessels;
- Class B uses the Carrier Sense Time Division Multiple Access (CSTDMA) scheme. It is used for lighter commercial and leisure vessels with its 2 watts transmission power;
- Base station, situated at the shore side, provides AIS channel management, time synchronization, text messages, navigation information, and meteorological and hydrological information;
- Aids to Navigation (AtoN), a shore- or buoy-based transceiver, is designed to collect and transmit data related to sea and weather conditions and to relay AIS messages so as to extend the network coverage;
- Search and rescue transceiver (SART), an emergency distress beacon that assists in homing to itself (i.e., lifeboats and life rafts). It transmits a text broadcast using message type 14.

The AIS uses the Time Division Multiple Access (TDMA) channel access method, which means the time unit is divided into many slots [9]. Generally, each time slot or frame can accommodate a single AIS message. A frame is 256 bits, and the standard data transmission rate is 9,600 bits/second. Therefore, each frame has a timing limit of 26.66 milliseconds, which results in 2,250 slots per minute per channel or 4,500 slots per minute in both channels. Sometimes, multiple frames can be used for a single message. AIS frames are transmitted into the air using Gaussian Minimum Shift Keying (GMSK) modulation with the bandwidth-time (BT) product set at 0.4. The data must be encoded using the Non-Return to Zero Inverted (NRZI) format before transmission. Figure 2 shows the basic structure of an AIS frame.

Ramp up 8 bit	Preamble 24 bit	Start flag 8 bit	Payload 168 bit	CRC 16 bit	Stop flag 8 bit	Buffer 24 bit

FIGURE 2. The basic structure of an AIS frame.

There are 64 types of AIS messages, of which 27 are currently in use. The rest (37) are reserved for the future. Some of the most important AIS message types are listed below.

- 1 = Position report of class A
- 4 = Base station report
- 14 = Safety-related broadcast message
- 18 = Standard class B position report
- 20 = Data link management message
- 21 = Aid-to-Navigation report
- 22 = Channel management
- 23 = Group assignment command
- 24 = Static data report

The full list and details of the AIS message types are available in [10]. Despite offering many valuable services for ship navigation, AIS falls short in security measures. Its main problem is that it does not utilize authentication or encryption; therefore, any attacker with the proper knowledge of generating valid AIS protocol signals can impact the AIS communication.

III. RELATED STUDIES

Mathapo [11] implemented an SDR-based AIS receiver as a proposed payload of the South African ZA-002 satellite in 2007. The proposed receiver can be used to track and store the movement of ships at sea and then forward this information to the ground station upon request. C++ programming language was used to implement the AIS receiver on the SDR architecture. The SDR AIS receiver was capable of high-pass filtering, amplifying, symbol synchronizing, decoding, bit destuffing, error checking, translating, and interpreting the AIS messages in real time. The results showed that the AIS messages were decoded correctly. Larsen *et al.* [12] also demonstrated their SDR-based AIS receiver for the Danish AAUSAT3 satellite. The receiver down-converts a 200KHz-wide frequency spectrum of around 162 MHz to a 200 KHz intermediate frequency (IF) signal, then samples it to an in-phase and quadrature components (IQ) signal at a speed of 1 mega-samples-per-second. Later, the IQ data is filtered into the two AIS channels. Then each channel is demodulated using matched filter implementation. The transmitted bits are estimated by recovering the bit-synchronization using a correlator to find the training sequence. The authors tested their receiver using a stratospheric balloon flight at a 24km altitude. The test results showed that AIS can be received from approximately 500km away. The first SDR-based AIS attacks were demonstrated in 2014 by Balduzzi *et al.* [6]. The authors developed a Python language-based program called *AISTX* [13] to create an AIS payload according to the protocol. GNU Radio Companion (GRC) was used to generate the IQs of the signal, which were transmitted into the air using the Universal Software Radio Peripheral (USRP). Three different receivers verified the reception of the counterfeit transmission. The AIS protocol specifications were affected by several threats and were vulnerable to cyberattacks such as spoofing, false collision threat, and service availability disruption.

Marques *et al.* [14] built a low-cost AIS transponder using a HackRF. The authors encoded the message with [15] and used *AISTX* to construct the final AIS frame. They tested the transmission of type 1 messages via an RF link. Another SDR-based receiver with a chart-plotting software called OpenCPN was used to test the reception. The main

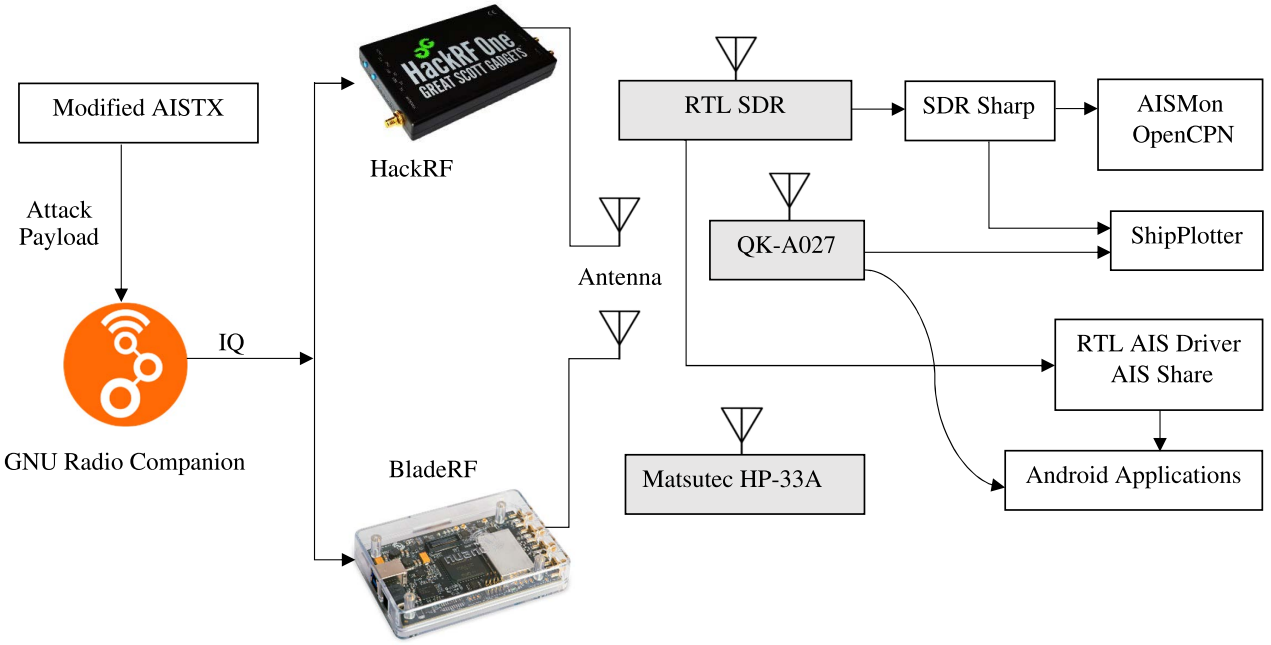


FIGURE 3. Experimental attack setup.

intention of their research was to develop a low-cost (around 150 euros) AIS transponder. A similar test was conducted by Cruz *et al.* [16]. Using transmission-enabled SDR, GRC, and *AISTX*, the authors transmitted the position of a ship. At the receiver end, they calculated the difference between the transmitted data and the received data. They found on average 7-meter difference in the ship's location between the original data and the received data. They found that the technical standard requires four decimal places in latitude and longitude, but the GPS device that they used provided three decimal places, which caused a small calculation error. Foster [17] developed an AIS decoder based on the Python programming language to report the shipborne position called "gr-ais". It can be used with GRC and other chart-plotting software. The software can be used with any SDR that provides IQ data, such as RTL-SDR and HackRF. Some other decoders were also developed [18], [19]. Attacks on ships are not limited to fake AIS transmissions. A research team from the University of Texas hijacked an $80 million yacht with cheap GPS spoofing [20]. In another test, the GPS spoofing resulted in an unbelievable ship speed [21]. Androjna *et al.* [22] studied AIS vulnerabilities and challenges. They thoroughly analyzed a spoofing event that happened near Elba in December 2019. The fake signals created a dangerous situation for a real ship. More than a dozen fake ships were found on a collision course of that ship. They concluded that the maritime industry is neither immune to cyberattacks nor fully prepared for the risks associated with the use of modern digital systems.

So far, only Balduzzi *et al.* [6] in 2014 have demonstrated attacks using AIS packet data. Other studies focused on the SDR implementation of AIS, decoding, or possibilities for cheap transponder build-up. Technology has drastically changed since the study of Balduzzi *et al.* [6] study. Many new types of receivers, software, chart-plotting applications using smart devices have been developed. Attackers have new tools and ideas as well. Therefore, evaluating the attacks on modern AIS setups against current technology is essential.

TABLE 1. List of hardware.

Hardware	Functionality
Matsutec HP-33A	Stand alone AIS transponder with GPS reception
Quark-elec QK-A027	AIS receiver. Share AIS data via USB and WiFi
RTL-SDR	AIS signal receiver
HackRF	Generate fake AIS RF signal
BladeRF	Generate fake AIS RF signal
Samsung A 21s	Navigation applications' host

IV. EXPERIMENT SETUP

Many types of AIS hardware and software are available in the market. Some hardware has built-in display functionality, while others display the AIS data through external software and additional accessories. In most cases, we found the hardware and software are interoperable. For the purpose of our study, a compatible combination of hardware and software makes an AIS setup for the evaluation. In this study, a total of 19 combinations of AIS setups were tested against AIS attacks. The hardware and software were selected

TABLE 2. List of software.

Software	Platform	Functionality
OpenCPN v 5.2.4	Windows	Displaying AIS data
iRegatta v 4.07	Android	Displaying AIS data
Ships v 4.07	Android	Displaying AIS data
Boating v 17.0.2	Android	Displaying AIS data
iBoating v 190.0	Android	Displaying AIS data
Boat Beacon v 2.53	Android	Displaying AIS data
AF track v 12.7	Android	Displaying AIS data
OpenCPN v 1.0.5	Android	Displaying AIS data
SDR sharp v 1.0.0.1732	Windows	Receiving AIS signal
RTL AIS driver v 1.1.8	Android	Decoding AIS data
AIS share v 1.2.2	Android	Sharing AIS data
ShipPlotter v 12.5.4.6	Windows	Decoding and displaying AIS data
AISmon v 2.2.0	Windows	Decoding and sharing AIS data

comprehensively to test the attacks on diverse AIS setups, yet at the same time the diversity of the setups was limited by the budget limitations, as well as market availability of certain products at the time of the experiments. The list of hardware and software used and their functionalities are presented in Tables 1 and 2, respectively. For this experiment, we have also acquired an official MMSI number from TRAFICOM (Finland). For privacy and safety reasons, we blurred the MMSI number in some figures. Some past studies used *AISTX* as an AIS payload generator. The original version of *AISTX* produced a single AIS frame at a time, when testing of some attacks such as DoS or flooding it was very slow. For the demands of this study, we modified *AISTX* so that it could produce *N* number of AIS frames from a single command in a single file. Linux-based GRC was used to produce the IQ samples based on the data of the file. Finally, the IQ samples were provided to the HackRF and BladeRF for the transmission of an AIS RF signal. To verify the reception and impact of the attacks, we used the Matsutec HP-33A AIS transponder, Quark-elec QK-A027 AIS receiver, Windows-based ShipPlotter [23] and OpenCPN [24] software, and several Android mobile applications. Apart from the HP-33A transponder which is an all-in-one complete setup, all other setups used QK-A027 and RTL-SDR as the RF front-end. In Windows, we used SDR Sharp to tune the AIS frequency and provided the resulting audio to AISMon [25], which decoded the AIS signal. The signal was subsequently fed to the OpenCPN using a UDP port in the National Marine Electronics Association (NMEA) format. ShipPlotter had a built-in decoder. In Android, the decoding task was done by the RTL AIS driver application. The decoded messages were shared by AIS Share with different navigation applications [26]. The QK-A027 receiver has a built-in decoder and could provide the decoded AIS data to the other application using a TCP port. Therefore, while QK-A027 was used, the Android applications did not need other decoding software. *Ships v 4.07* did not work with QK-A207 because that application does not support a TCP connection. Figure 3 shows the experimental attack setup and how the AIS payload reaches the receiver over the air. Modified *AISTX* supplied the payload to GRC, where base-band IQs of the signal are generated according to the GMSK modulation. The IQs are transmitted into the air using HackRF and BladeRF. AIS receivers receive the signal from the air and demodulate, decode, and display the AIS data. Figure 4 shows the GRC transmission script. We maintained the 9,600 bits-per-second rate according to the AIS protocol. Therefore, 2 mega-samples-per-second resulted in around 208 samples/symbol. The bandwidth-time is the product of the duration of a signal and its spectral width, which was set at 0.4. By changing the channel frequency, we were able to transmit on both AIS channels. Moreover, through multiple transmission-enabled SDRs, we were able to simultaneously transmit the AIS signal in both channels.

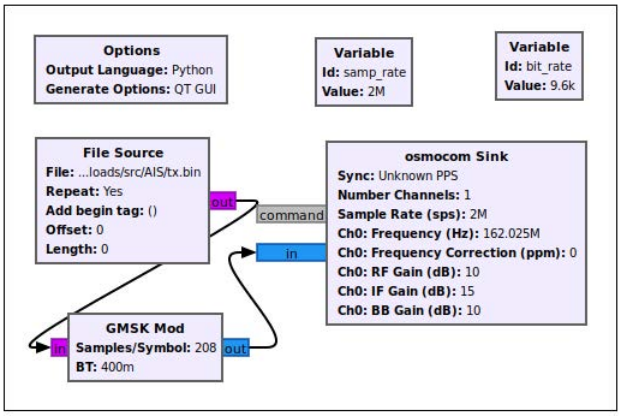


FIGURE 4. GRC flow-graph for AIS injections.

V. ATTACKS AND RESULTS

This section describes different types of attacks on AIS and the observed impact on the receiving devices and applications.

A. SPOOFING

We were able to produce spoofed or fake ships, as has already been done before [6]. The spoofed ship was visible on all the receivers, including the commercial AIS transponder. A spoofed ship may have severe consequences [3] and may jolt the safety of navigation in waterways. Figure 5 shows a spoofed ship.

B. MAN OVERBOARD

Man Overboard (MOB) is a survivor recovery alert system used when a crew member or a passenger falls off the ship into the water or used by rescue workers in any ship evacuation operation. It indicates that a human is in the water and needs immediate rescue. It is a small beacon that transmits to the neighboring vessels a distress AIS signal containing the beacon's GPS location (if available). The MOB signal

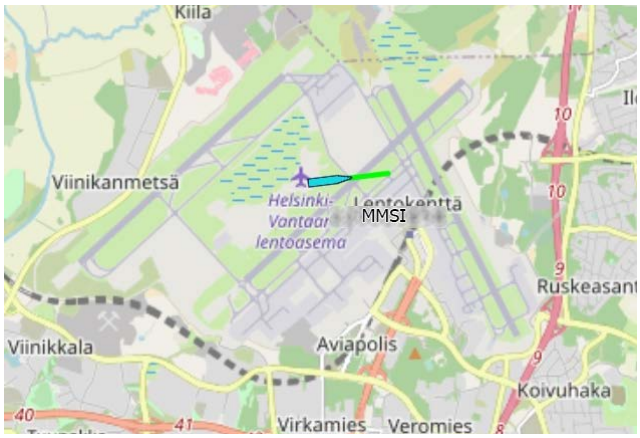


FIGURE 5. A spoofed maritime vessel as-if present on the runway of Helsinki airport in an android ship application.

uses a type 1 message, navigation status 14, and a 9-digit MMSI starting with 972. It alerts the ship's radar system that there is an emergency. Using our aviation and maritime pentesting platform, we were able to produce a fake MOB alert. Attackers using this type of counterfeit signal can waste a significant amount of time of any ship by engaging the ship in a vain and costly rescue operation. Figure 6 shows a MOB alert in the Matsutec HP-33A transponder due to the fake distress signal.

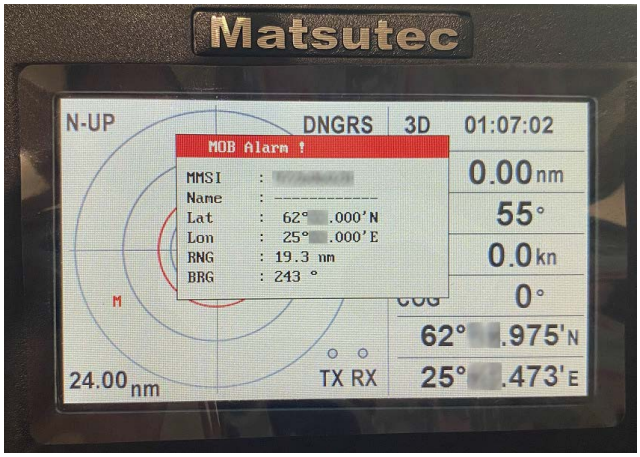


FIGURE 6. MOB alert in the Matsutec HP-33A AIS transponder.

C. COLLISION ALERT

Since it is possible to fake a ship's location, we placed a fake ship near another ship to observe the reaction. We observed that when the closest point of approach (CPA) and the time to the closest point of approach (TCPA) values fell behind the threshold, the ship was alerted about a possible collision. Attackers may use this type of attack to change the course of a target vessel. Figure 7 shows a collision alert.

FIGURE 7. Collision alert in ShipPlotter.

D. JAMMING

Jamming in AIS can be divided into two categories: RF jamming, and (display) flooding. RF jamming is the transmission of overpowered white noise to the AIS channels in such a way that the valid packets cannot be transmitted through the channel. We tested RF jamming in our laboratory. Although it worked, the effectiveness of this type of attack in vast water areas would be limited. We were able to jam the channels with valid AIS packets. According to the AIS's TDMA scheme, each AIS channel has 2,250 available time slots to receive AIS signals from a maximum of 2,250 different ships every minute. Each unique MMSI is counted as a different ship. Using the modified *AISTX*, we generated two files that contained a huge amount of AIS frames with different MMSI. Using two transmission-enabled SDRs, we transmitted those two files to both AIS channels. Figure 8 shows a screenshot of the AIS reception statistics in the AIS Share application. Two consequent attackers using SDRs consumed approximately 96% of channel A's capacity and 100% of channel B's capacity. Thus, the channels can be jammed by the attacker with valid messages.

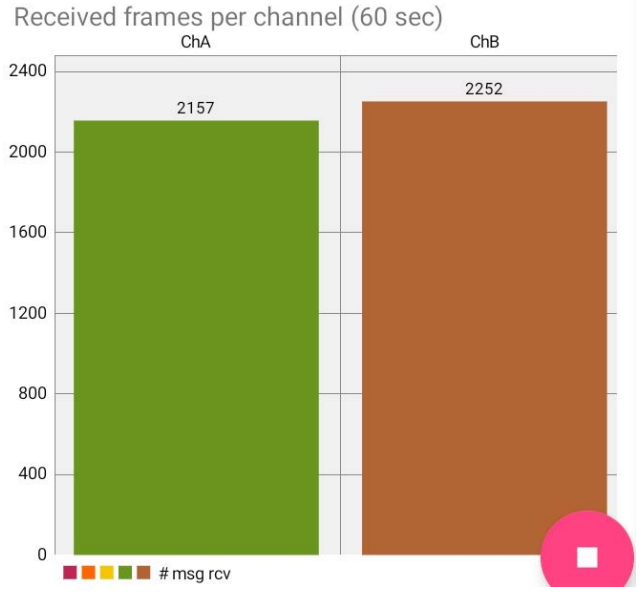


FIGURE 8. Signal receiving statistics of both channels for one minute in AIS Share.

E. OVERWHELMING ALERTS

Usually, AIS receivers raise an alert when there is a possibility of collision with another ship based on the CPA and TCPA thresholds or in a distress situation like MOB. We took

advantage of this feature to trigger a huge number of alerts in a short period of time. We set 1,000 fake ships very near the receiver's *Own ship* location to trigger the collision alert. Similarly, in another test, we transmitted 1,000 MOB distress signals. We found that a large number of simultaneous alerts led to a crash of the ShipPlotter software, which did not crash under normal circumstances when exposed to the AIS DoS attack (see V-I). When an overwhelming number of collision alerts, similar to Figure 7, started to pile up on the user interface, the software eventually collapsed, hence affecting the availability of a mission-critical software and display. Some applications do not present any alert at all, which is quite dangerous and exposes the ship to unnecessary risk. Relying on this type of poor software may lead to accidents and other unexpected scenarios. We also noticed that the overwhelming number of alerts lead to a situation in some software where thousands of audio-visual alerts create a chaotic situation called ''alert fatigue'' [27]. A true positive alert may go unnoticed in such a chaotic situation. Table 3 summarizes the result of our alert-handling tests. Certainly, similarly to traffic collision avoidance system (TCAS) and cockpit systems [28], the AIS users (e.g., port and ship crews) may switch off the AIS receivers in case of malicious attacks via overwhelming alerts. However, such switching off, in essence, means the AIS is under DoS, and the entire benefits of AIS (e.g., navigational awareness and communication) is completely lost.

F. COORDINATED ATTACK

Among the data fields in an AIS message, the MMSI number is used as the main reference by the receiving software. In successive messages, information on a particular ship is updated against this MMSI number. To avoid a conflict with other ships' MMSIs, some commercial transponders allow the MMSI to be set only once. However, since our pentesting platform can use any MMSI number, multiple emitters can be used to transmit different AIS signals containing the same MMSI number. During this type of attack, the attackers coordinate among themselves to send multiple signals that contain the same reference (the MMSI number) but differing values in some of the AIS data fields. This is called a ''coordinated attack.'' Since the reference point is the same, the data fields will be updated according to the encoded message of multiple signals in the receiving software. However, some fields in AIS should be updated by following a standard or a common pattern. For example, the position of the ship should be updated smoothly with a clear course, possibly with a historical fading-out path. However, in a coordinated attack, the attackers, using multiple emitters, can change the position of the ship from one place to another in an instant. Cargo carriers may turn into passenger carriers. The ship's name, call sign, dimension, and other data may differ in a second. These can lead to confusion in Vessel Traffic Services (VTS) or among other ships, thus producing dangerous consequences. We focused on the most important data fields of AIS, for example, the ship name, call sign, position, speed, navigation status, vessel type, and dimension. We observed that in all the receivers, the ship's information fluctuates every second, that is, alternates between different transmitters' signal values. Table 4 shows the results of the coordinated attack. In practice, it is possible to carry out a coordinated attack even with a single attacking emitter since the legitimate ship itself can be the second emitter. In this case, the attacking emitter mimics the target ship's MMSI number and alters the other values, thus achieving effects similar to those when there are two coordinated attackers.

TABLE 3. Test results: overwhelming alerts.

Configuration		Observation	
Hardware	Software	Collision alert	MOB alert
Matsutec HP-33A	Matsutec Firmware v 1.0	All alerts in a list with one audio alert	All alerts in a list with one audio alert
RTL-SDR	ShipPlotter v 12.5.4.6	Many audio and visual alerts prompted to a software **crash**	**No alert**
	OpenCPN v 5.2.4	**Alert fatigue**	**Alert fatigue**
	iRegatta v 4.07	**No alert**	**No alert**
	Ships v 4.07	**No alert**	**No alert**
	Boating v 17.0.2	**Alert fatigue**	Red color MOB locations and one audio alert
	iBoating v 190.0	**No alert**	**No alert**
	Boat Beacon v 2.53	**Alert fatigue**	**Alert fatigue** Red color MOB locations
	AF track v 12.7	**No alert**	Red color MOB locations
	OpenCPN v 1.0.5	**Alert fatigue**	**Alert fatigue**
QK-A027	ShipPlotter v 12.5.4.6	Many audio and visual alerts prompted to a software **crash**	**No alert**
	OpenCPN v 5.2.4	**Alert fatigue**	**Alert fatigue**
	iRegatta v 4.07	**No alert**	**No alert**
	Ships v 4.07	Did not work	Did not work
	Boating v 17.0.2	**Alert fatigue**	Red color MOB locations and one audio alert
	iBoating v 190.0	**No alert**	**No alert**
	Boat Beacon v 2.53	**Alert fatigue**	**Alert fatigue** Red color MOB locations
	AF track v 12.7	**No alert**	Red color MOB locations
	OpenCPN v 1.0.5	**Alert fatigue**	**Alert fatigue**

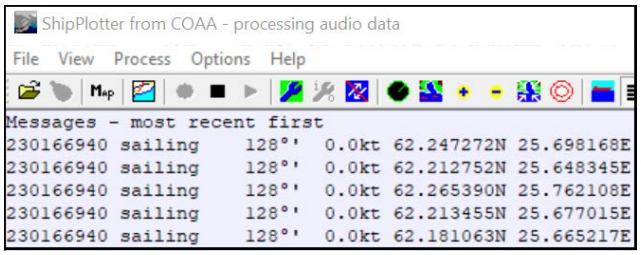
G. LOGICALLY INVALID DATA ENCODING

We noticed that there is no data validity checking in AIS. It is possible to form technically correct but logically invalid messages. For example, in Figure 9(a), ShipPlotter decodes that a ship (with the same MMSI number) went from one place to another place, but its speed remained zero even though it was sailing. This type of irrationality among data may open the opportunity for an attack. For example, if the speed remains zero, a TCPA alert would not be triggered. Figure 9(b) shows that multiple ships engaged in different activities have different speeds and courses, but all of them have the same name and call sign. Such a situation could be confusing for VTS or other ships if the MMSI is not checked carefully. However, maintaining the same MMSI number through a coordinated attack can result in a more complex situation, which we describe in V-F. Nonetheless, for these logically invalid data, no receiver provided any alarm during our experiment.

TABLE 4. Test results: coordinated attack.

Configuration		Effects						
Hardware	Software	Ship name	Call sign	Vessel type	Navi. status	Speed	Position	Ship dimension
Matsutec HP-33A	Matsutec Firmware v 1.0	FLC	FLC	FLC	FLC	FLC	FLC	FLC
RTL-SDR	ShipPlotter v 12.5.4.6	FLC	FLC	FLC	FLC	FLC	FLC	FLC
	OpenCPN v 5.2.4	FLC	FLC	FLC	FLC	FLC	FLC	FLC
	iRegatta v 4.07	FLC	INA	INA	INA	FLC	FLC	INA
	Ships v 4.07	FLC	FLC	FLC	FLC	FLC	FLC	FLC
	Boating v 17.0.2	FLC	FLC	INA	FLC	FLC	FLC	FLC
	iBoating v 190.0	FLC	FLC	FLC	FLC	FLC	FLC	FLC
	Boat Beacon v 2.53	FLC	INA	FLC	FLC	FLC	FLC	FLC
	AF track v 12.7	FLC	FLC	FLC	FLC	FLC	FLC	FLC
	OpenCPN v 1.0.5	FLC	FLC	FLC	FLC	FLC	FLC	FLC
QK-A027	ShipPlotter v 12.5.4.6	FLC	FLC	FLC	FLC	FLC	FLC	FLC
	OpenCPN v 5.2.4	FLC	FLC	FLC	FLC	FLC	FLC	FLC
	iRegatta v 4.07	FLC	INA	INA	INA	FLC	FLC	INA
	Ships v 4.07	DNW	DNW	DNW	DNW	DNW	DNW	DNW
	Boating v 17.0.2	FLC	FLC	INA	FLC	FLC	FLC	FLC
	iBoating v 190.0	FLC	FLC	FLC	FLC	FLC	FLC	FLC
	Boat Beacon v 2.53	FLC	INA	FLC	FLC	FLC	FLC	FLC
	AF track v 12.7	FLC	FLC	FLC	FLC	FLC	FLC	FLC
	OpenCPN v 1.0.5	FLC	FLC	FLC	FLC	FLC	FLC	FLC

Note: FLC = Fluctuates (i.e., displays alternate values from different attackers); INA = Information Not Available in the application; DNW = Did Not Work.



(a)

AIS target list

MMSI	Name	Call	SoG	CoG	Type	Nav Status
[redacted]	ABC	XYZ123	39.9	350	Tanker	Under way sailing
[redacted]	ABC	XYZ123	96.9	262	Cargo Ship	High Speed Craft
[redacted]	ABC	XYZ123	40.1	301	Passenger Ship	Power-driven vessel

(b)

FIGURE 9. (a) Zero speed ship moving position in ShipPlotter. (b) Different ships having the same Name and call sign in OpenCPN.

H. VISUAL NAVIGATION DISRUPTION

Ships generally navigate in water by following an AIS-supported plotted chart or radar screen. We found that this visual navigation can be significantly disrupted by fake AIS transmissions. For example, message type 4 is reserved for the AIS base station, which is usually stationary on the shore. However, in some type 4 messages, we changed the coordinate value linearly but kept the same MMSI, so it appeared that the base station was moving towards the ship along the navigation line of the ship itself. In another setting, using several different MMSI and geo-coordinate values, we surrounded a ship with stationary base stations. Figure 10 shows a scenario wherein a ship is surrounded by base stations. This type of situation may cause the operator of the ship to experience serious situational awareness confusion.

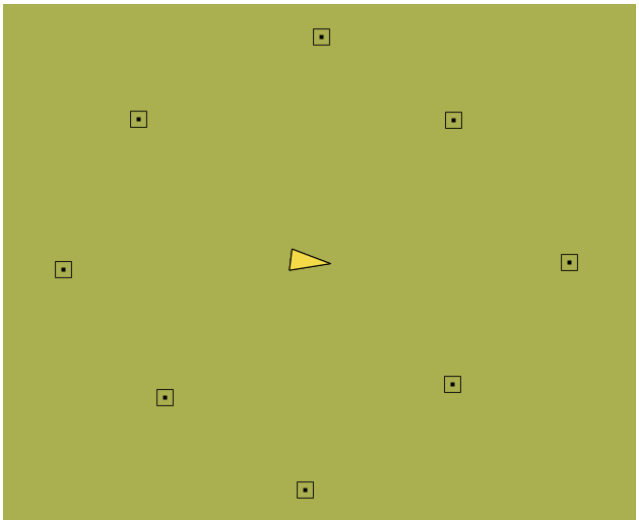


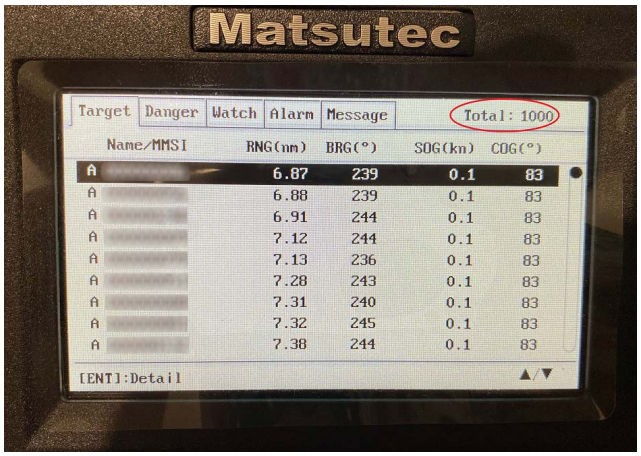
FIGURE 10. Ship surrounded by fake base stations in OpenCPN.

I. DENIAL OF SERVICE

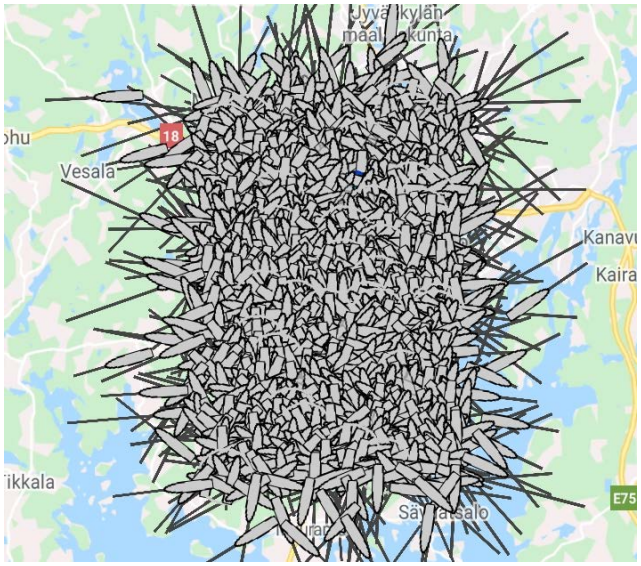
To test the system resiliency, we performed our DoS attack by trying to "overpower" the receivers with AIS signals. Our modified *AISTX* could produce *N* number of AIS frames at a time. We produced 200K type 1 frames in a single file and transmitted it through an SDR. The results in Table 5 show that approximately 89% of the configurations were impacted by the DoS attack (e.g., the output was clogged, unresponsive, or crashed). Some software did not crash during the AIS DoS attack because they decoded only a limited number of distinct MMSIs (e.g., up to 1,000 for Matsutec HP-33A). However, this type of behavior indicates the possibility of a legitimate message drop. Some setups follow a moderate decoding cycle to optimize memory and displaying capacity. However, the attack floods the display, so it becomes nearly impossible to read the screen. Figure 11(a) shows that the Matsutec transponder was clogged at its maximum decoding capability of 1,000 ships. Figure 11(b) shows the flooded screen of an Android application.

J. ERROR HANDLING TEST

According to the technical characteristics of AIS, cyclic redundancy check (CRC) is used for error detection [9]. If an error is detected, that message is dropped, assuming possible corruption. To test the error detection system, we deliberately flipped a message bit and repeatedly transmitted that file with a HackRF. We observed that all the receivers dropped the erroneous message. Figure 12 shows the error detection in AISMon, where all the messages were detected as erroneous messages. Error detection worked well across all the tested setups. However, none of them alerted the user regarding the erroneous packets. Error correction and alerting are optional in the standard. For many reasons, an error can occur; for example, we found that sometimes, due to a slight frequency offset in the receiver, a valid AIS frame was regarded as invalid. Alerting users upon error detection could help them to



(a)



(b)

FIGURE 11. (a) Clogged screen as effect of AIS DoS attack on Matsutec HP-33A. (b) Flooded screen as effect of AIS DoS attack on boat beacon.

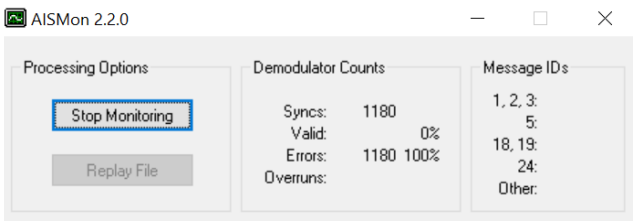


FIGURE 12. Detection of errors in AIS frames by AISMon.

calibrate the system for better-quality service. Moreover, in a congested RF channel, signal distortion is a regular incident, which can induce an error. Therefore, besides error detection, ADS-B uses an error correction system. An error correction scheme can save significant RF pollution. Thus we suggest at least a 1-bit error correction system in AIS.

K. AIS PREAMBLE TEST

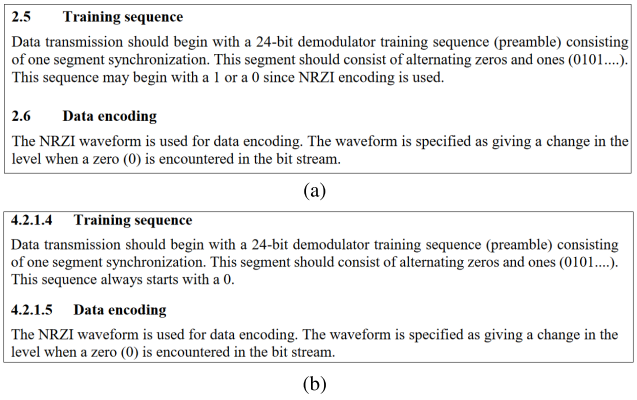
During some early experiments, we noticed that one of our testbed devices (QK-A027) misbehaved. It displayed data from some transponders (e.g., Matsutec) but did not display valid non-attack AIS signals from our pentest platform. At the same time, the same signal was displayed perfectly fine in the Matsutec-based and RTL-SDR-based setups. This prompted us to investigate further this root cause of the QK-A027's misbehavior, which led us to discover what we call the "AIS preamble-related implementation flaw".

AIS uses a 24-bit preamble consisting of alternating zeros and ones (0101….). ITU-R M.1371-5 [9] in Annex 2 titled "Technical characteristics of an automatic identification system using time division multiple access techniques in the maritime mobile band" (in Figure 13(a)) specifies that the preamble (or training sequence) can start with 1 or 0 when transmitting. At the same time, the same document in Annex 7 titled "Class B automatic identification system using carrier sense time division multiple access technology" (in Figure 13(b)) specifies that the preamble always starts with 0 when transmitting. Annex 2 focuses on the SOTDMA channel access scheme, which is mainly used by class A vessels, while Annex 7 focuses on the CSTDMA scheme

TABLE 5. Test results: DoS attack.

Configuration		Observation
Hardware	Software	
Matsutec HP-33A	Matsutec Firmware v 1.0	**Output clogged** Maximum 1,000 MMSI displaying capacity
RTL-SDR	ShipPlotter v 12.5.4.6	No impact
	OpenCPN v 5.2.4	**Unresponsive** After approx. 30 minutes
	iRegatta v 4.07	**Crashed**
	Ships v 4.07	**Unresponsive** After approx. 20 minutes
	Boating v 17.0.2	**Output clogged** Maximum 100 MMSI displaying capacity
	iBoating v 190.0	**Output clogged** Maximum 1,200 MMSI displaying capacity
	Boat Beacon v 2.53	**Unresponsive** After approx. 20 minutes. Crashed sometimes.
	AF track v 12.7	**Output clogged** Approx. 11 minutes decoding cycle. Remove old decoded data when new cycle starts.
	OpenCPN v 1.0.5	**Unresponsive** After approx. 10 minutes. Crashed sometimes.
QK-A027	ShipPlotter v 12.5.4.6	No impact
	OpenCPN v 5.2.4	**Unresponsive** After approx. 30 minutes
	iRegatta v 4.07	**Crashed**
	Ships v 4.07	Did not work
	Boating v 17.0.2	**Output clogged** Maximum 100 MMSI displaying capacity
	iBoating v 190.0	**Output clogged** Maximum 1,200 MMSI displaying capacity
	Boat Beacon v 2.53	**Unresponsive** After approx. 20 minutes. Crashed sometimes.
	AF track v 12.7	**Output clogged** Approx. 11 minutes decoding cycle. Remove old decoded data when new cycle starts.
	OpenCPN v 1.0.5	**Unresponsive** After approx. 25 minutes. Crashed sometimes.

primarily used for class B vessels. Nonetheless, according to the requirement [9], regardless of class, all the vessels (in the range) should be visible to each other via AIS. Therefore, the International Electrotechnical Commission (IEC) standards IEC 62287-1 [29], IEC 62287-2 [30], and IEC 61993-2 [31] require all *Equipment Under Test* to receive the signal regardless of where the preamble starts with 0 or 1. Now, allowing the transmission preamble to start with 1 and expecting the reception preamble to start with 0 may induce confusion. The QK-A027 case can be an example. We observed that the QK-A027 receiver did not receive messages when the preamble in the messages started with 1. However, it detected the message when the preamble started with 0. The details of the AIS preamble test are presented in Table 6.



2.5 Training sequence

Data transmission should begin with a 24-bit demodulator training sequence (preamble) consisting of one segment synchronization. This segment should consist of alternating zeros and ones (0101....). This sequence may begin with a 1 or a 0 since NRZI encoding is used.

2.6 Data encoding

The NRZI waveform is used for data encoding. The waveform is specified as giving a change in the level when a zero (0) is encountered in the bit stream.

(a)

4.2.1.4 Training sequence

Data transmission should begin with a 24-bit demodulator training sequence (preamble) consisting of one segment synchronization. This segment should consist of alternating zeros and ones (0101....). This sequence always starts with a 0.

4.2.1.5 Data encoding

The NRZI waveform is used for data encoding. The waveform is specified as giving a change in the level when a zero (0) is encountered in the bit stream.

(b)

FIGURE 13. (a) AIS preamble instruction in ITU-R M.1371-5, Annex 2. (b) AIS preamble instruction in ITU-R M.1371-5, Annex 7.

Certainly, the way the specification is drafted and the lack of cautionary notes can easily mislead system designers, developers, and integrators. This finding would mean in practice that there is a very high probability that a ship equipped with a QK-A027 may not detect some other ships on the AIS displays. Therefore, this could lead to a possible collision or a similar accident, especially in low-visibility situations. Moreover, this problem is not necessarily isolated to QK-A027. In fact, we fear that similar misinterpretations and implementation flaws could have been made by other vendors or in other models similar to QK-A027 from the same vendor. In practice, this means that extensive retesting and revalidation of a large number of devices are required, with particular application of the methodology proposed in this article. While investigating this issue, we also studied the impact of NRZI conversion on the AIS data and preamble. We present those results in Appendix A for technical completeness.

VI. DEFENCE AGAINST AIS ATTACKS

Attacks on AIS can affect information confidentiality, authenticity, integrity, availability, possession, and utility [32], which need to be prioritized. However, implementing a proper defense strategy requires more systematic research

TABLE 6. AIS signal detection status depending on the preamble start.

Configuration		Preamble	
Hardware	Software	Starts with 1	Starts with 0
Matsutec HP-33A	Matsutec Firmware v 1.0	✓	✓
RTL-SDR	ShipPlotter v 12.5.4.6	✓	✓
	OpenCPN v 5.2.4	✓	✓
	iRegatta v 4.07	✓	✓
	Ships v 4.07	✓	✓
	Boating v 17.0.2	✓	✓
	iBoating v 190.0	✓	✓
	Boat Beacon v 2.53	✓	✓
	AF track v 12.7	✓	✓
	OpenCPN v 1.0.5	✓	✓
QK-A027	ShipPlotter v 12.5.4.6	×	✓
	OpenCPN v 5.2.4	×	✓
	iRegatta v 4.07	×	✓
	Ships v 4.07	–	–
	Boating v 17.0.2	×	✓
	iBoating v 190.0	×	✓
	Boat Beacon v 2.53	×	✓
	AF track v 12.7	×	✓
	OpenCPN v 1.0.5	×	✓

and development, which is beyond the core focus of this paper. Nonetheless, in a similar service in aviation (ADS-B), we showed a received signal strength (RSS) and distance relationship model [8] that reached up to 90% accuracy in the best case. This strategy can easily be transferred to AIS, as the concept is protocol agnostic. We cannot create yet an RSS-Distance model for the AIS service because we are not in the close vicinity of a real-world port where realistic AIS traffic is seen. In fact, from our location (the central part of Finland), we do not receive any AIS messages. In the current literature, researchers have suggested some solutions.

To identify erroneous transmissions or falsified data, Ray *et al.* [33] proposed checking the integrity of the AIS data. According to them, the integrity can be assessed by comparing the AIS data with long-term historical data on the message with respect to other messages, and on the signal itself with its physical characteristics. Their proposed method is supposed to provide an integrity-based confidence coefficient on data that can be used to take further action on that data.

Junior *et al.* [34] showed a triggering mechanism that uses an image processing template matching technique to detect specific patterns transmitted by an attacker. Chart plotter software (e.g., OpenCPN) plots the ship on the map as it receives the data through AIS. This plotting changes the mean

intensity of the pixels of an area on the map. The authors set a threshold and compared the display pixel intensity; if it exceeded the threshold, it triggered the alerting mechanism. The authors reported a 93% success rate.

Goudossis and Katsikas [35] proposed identity-based public cryptography and symmetric cryptography to enhance the security of AIS. For asymmetric cryptography, they proposed that IMO generate a private key for the corresponding public keys of the National Maritime Authorities (NMA). In contrast, NMA could generate private keys for the corresponding keys at the national level. They also proposed symmetric cryptography for insecure sea areas such as the coast of Somalia. In this case, the presence of at least one trusted third party (e.g., a military patrol boat or a micro-satellite) is necessary to create and distribute the keys.

Bothur *et al.* [36] analyzed the security vulnerabilities and countermeasures in a smart ship system. According to them, most of the electronics systems in a ship, such as information technology networks, control systems, electronic chart display information system, very small aperture terminals, and AIS, are vulnerable to cyberattacks. They listed the possible weakness of all the subsystems. They mentioned that proper policy, and ensuring the security of data, application, host, network, etc., could help counter the attacks.

Su *et al.* [37] proposed a digital certificate-based identity authentication scheme to ensure the authenticity of the AIS data. According to them, a ship should generate its public and private keys. The public key should be distributed by an trusted official institution. They further proposed a mixed-zone and blind-signature-based trajectory privacy protection scheme to protect the vessel identity and the trajectory privacy. They suggested using pseudonyms instead of the actual MMSI to safeguard the true identity of a ship under the supervision of a trusted party called a ''certification authority'' (CA). It knows the relationship of every pseudonym to the real identity. If ships want to bar the CA from knowing the identity of the ship, the selection of pseudonyms must be executed by the vessel. In this case, the vessel sends many digital signatures to the CA. After the CA signs and returns the signatures, the ship chooses one randomly.

Sciancalepore *et al.* [38] proposed a secure, flexible, standard-compliant, and backward-compatible authentication framework to secure AIS broadcast messages. They contextualized a broadcast authentication protocol called Timed Efficient Stream Loss-tolerant Authentication (TESLA) and a space- and time-efficient probabilistic data structure called ''Bloom filter data structure'' in their authenticated AIS called ''Auth-AIS.'' Their proposed system required transmission of cryptography-related data via a type 8 message, which increases the AIS overhead. The difference with other cryptography solutions and Auth-AIS is the start time of the AIS transmission for a vessel, which is hidden but shared with other vessels by a trusted third party. An attacker is unlikely to know the precise AIS transmission timing of a vessel; thus, the fake transmission would not be authenticated by other ships.

VII. CONCLUSION

In this paper, we practically demonstrated and evaluated the impact of multiple attacks on AIS (both novel and known ones), primarily achievable via an RF link and with effects on the various network, processing, and display subsystems used within the AIS ecosystem. We developed a heterogeneous testbed that consisted of a commercial transponder, dual-channel AIS receiver, several SDRs, and software from different platforms (e.g., Android, Windows, and embedded OS), which resulted in a total of 19 tested configurations. Overall, within a controlled environment we performed 11 different tests/attacks, most of which represented either novel attack concepts or novel implementation of existing ideas in the AIS context. We demonstrated that the navigation security of multi-million dollar ships can be affected by a low-cost setup. Almost all the test configurations were impacted by some sort of attack. A coordinated attack, flooding, visual navigation disruption, and others indicate that attackers can be potentially harmful due to their ingenious attacks and state-of-the-art equipment. Software crashes due to DoS or an overwhelming number of alerts showed the most worrying scenario. Mobile applications are mostly unreliable and more vulnerable to attacks than desktop solutions, very likely due to memory, display, and computational constraints. During the experiments, we identified an AIS preamble-related implementation flaw. When the preamble started with 0, it worked fine across all the devices; but when it started with 1, it had the potential to affect the interoperability of some AIS devices. We urge the relevant stakeholders to pay attention to this issue to avoid further mishaps. Test results throughout this study reveal that, apart from the preamble-related issue, the other attack consequences belong to the software limitation. The identified issues are in the process of being reported to respective vendors according to responsible disclosure policy. The consistency of our results for a comprehensive range of hardware-software configurations indicates the reliability of our approach and test results. We hope researchers and industry can positively use our approach and outcomes to improve the cybersecurity of today's ever-growing AIS deployments. In the future, we plan to design, implement, and test different defense strategies against attacks on AIS. We also leave the jamming of specific messages for any targeted receiver as our future work.

APPENDIX A
AIS PREAMBLE AND NRZI

AIS uses NRZI encoding to encode the data. NRZI has many variants, and the one where the waveform changed due to the occurrence of 0 is called Non-Return-to-Zero Space (NRZS). More precisely, AIS uses NRZS variant of NRZI. Therefore, we also investigated the resulting differences between the scenarios where the preamble starts with 0, and 1 respectively, when using the NRZI conversion. Before the preamble starts according to the AIS message structure in Figure 2 there should be an 8-bit ramp up (*000000000*). Since NRZI depends on the previous level, we draw the signal with

ramp-up bits. The Figure 14 shows that after NRZI encoding, the two signals are not exactly the same. We further checked the NRZI conversion of AIS data with the Matlab code in [39]. That also resulted that preamble start with 1 and preamble start with 0 do not result exactly the same after NRZI conversion.

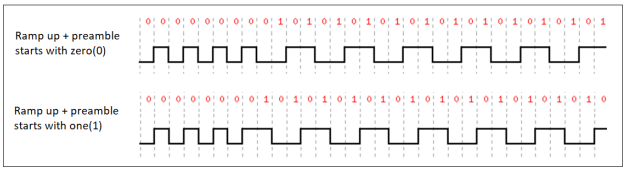


FIGURE 14. Comparison of NRZI conversion of ramp up and preamble bits – scenarios when starting with 0, and 1, respectively.

ACKNOWLEDGMENT

Some graphic materials in Figures 1 and 3 are under the fair-use courtesy of: GNU Radio, Nuand/Antratek, and HackRF/GreatScottGadgets; and royalty-free icons from www.flaticon.com (icons by: Freepik, Mattbadal, and Xnimrodx).

REFERENCES

[1] IMO. *AIS Transponders*. Accessed: Dec. 10, 2021. [Online]. Available: https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx
[2] *Vessel Finder*. Accessed: Dec. 11, 2021. [Online]. Available: https://www.vesselfinder.com/vessels
[3] T. Bateman. *HMS Defender: AIS Spoofing is Opening up a New Front in the War on Reality*. Accessed: Nov. 16, 2021. [Online]. Available: https://www.euronews.com/next/2021/06/28/hms-defender-ais-spoofing-is-o%pening-up-a-new-front-in-the-war-on-reality
[4] C. Zwirko. *North Korean Vessels Exploiting Tracking System Flaws to Evade Sanctions: Report*. Accessed: Nov. 15, 2021. [Online]. Available: https://www.nknews.org/2019/06/north-korean-vessels-exploiting-tracking%-system-flaws-to-evade-sanctions-report
[5] S. Chambers. *U.S. Warns Merchant Shipping of Iranian GPS Spoofing Threat*. Accessed: Nov. 15, 2021. [Online]. Available: https://splash247.com/us-warns-merchant-shipping-of-iranian-gps-spoofin%g-threat
[6] M. Balduzzi, A. Pasta, and K. Wilhoit, "A security evaluation of AIS automated identification system," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, Dec. 2014, pp. 436–445.
[7] A. Costin and A. Francillon, "Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," *Black Hat USA*, vol. 1, pp. 1–12, Jul. 2012.
[8] S. Khandker, H. Turtiainen, A. Costin, and T. Hamalainen, "Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures," *IEEE Trans. Aerosp. Electron. Syst.*, early access, Dec. 31, 2021, doi: 10.1109/TAES.2021.3139559.
[9] *Technical Characteristics for an Automatic Identification System Using Time-Division Multiple Access in the VHF Maritime Mobile Band*, International Telecommunication Union, Geneva, Switzerland, 2014. [Online]. Available: https://www.itu.int/rec/R-REC-M.1371-5-201402-I
[10] United States Coast Guard. *AIS Messages*. Accessed: Dec. 19, 2021. [Online]. Available: https://www.navcen.uscg.gov/?pageName=AISMessages
[11] K. F. Mathapo, "A software-defined radio implementation of maritime AIS," M.S. thesis, Dept. Elect. Electron. Eng., Univ. Stellenbosch, Stellenbosch, South Africa, 2007.
[12] J. A. Larsen, H. P. Mortensen, and J. D. Nielsen, "An SDR based AIS receiver for satellites," in *Proc. 5th Int. Conf. Recent Adv. Space Technol. (RAST)*, Jun. 2011, pp. 526–531.
[13] M. Balduzzi. *AISTX*. Accessed: Aug. 25, 2021. [Online]. Available: https://github.com/trendmicro/ais
[14] M. M. Marques, D. Teles, V. Lobo, and G. Capela, "Low-cost AIS transponder using an SDR device," in *Proc. OCEANS MTS/IEEE SEATTLE*, Oct. 2019, pp. 1–4.
[15] E. S. Raymond. *AIVDM/AIVDO Protocol Decoding*. Accessed: Dec. 28, 2021. [Online]. Available: https://gpsd.gitlab.io/gpsd/AIVDM.html
[16] F. R. G. Cruz, R. C. M. Gania, B. W. C. Garcia, and J. C. R. Nob, "Implementing automatic identification system transmitter on software defined radio," in *Proc. IEEE 10th Int. Conf. Humanoid, Nanotechnol., Inf. Technol., Commun. Control, Environ. Manage. (HNICEM)*, Nov. 2018, pp. 1–4.
[17] N. Foster. *Automatic Information System Decoder for Shipborne Position Reporting for the Gnuradio Project*. Accessed: Dec. 13, 2021. [Online]. Available: https://github.com/bistromath/gr-ais
[18] H. Hannikainen. *Open Source Software for Demodulating and Decoding AIS Messages*. Accessed: Dec. 19, 2021. [Online]. Available: https://github.com/rubund/gnuais
[19] A. D. Cruz. *Automatic Identification System (AIS) using GNU Radio*. Accessed: Dec. 30, 2021. [Online]. Available: https://www.funwithelectronics.com/?id=9
[20] B. Brewin. (2013). *University of Texas Team Hijacks $80 Million Yacht With Cheap GPS Spoofing Gear*. Accessed: Oct. 10, 2021. [Online]. Available: https://www.nextgov.com/cio-briefing/2013/07/university-texas-team-hija%cks-80-million-yacht-cheap-gps-spoofing-gear/67625
[21] M. L. Psiaki, T. E. Humphreys, and B. Stauffer, "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," *IEEE Spectr.*, vol. 53, no. 8, pp. 26–53, Aug. 2016.
[22] A. Androjna, M. Perkovič, I. Pavic, and J. Mišković, "AIS data vulnerability indicated by a spoofing case-study," *Appl. Sci.*, vol. 11, no. 11, p. 5015, May 2021.
[23] COAA. *ShipPlotter*. Accessed: Aug. 27, 2021. [Online]. Available: http://www.coaa.co.U.K./shipplotter.htm
[24] OpenCPN. *Chart Plotter and Navigational Software*. Accessed: Aug. 20, 2021. [Online]. Available: https://opencpn.org
[25] MarineTraffic. *AISMon*. Accessed: Nov. 17, 2021. [Online]. Available: https://help.marinetraffic.com/hc/en-us/articles/205339707-AISMon
[26] ebcTech. *AIS Share*. Accessed: Aug. 20, 2021. [Online]. Available: https://play.google.com/store/apps/details?id=eu.ebctech.ais_share&hl=e%n&gl=U.S
[27] W. U. Hassan, S. Guo, D. Li, Z. Chen, K. Jee, Z. Li, and A. Bates, "NoDoze: Combatting threat alert fatigue with automated provenance triage," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2019, pp. 1–40.
[28] M. Smith, M. Strohmeier, J. Harman, V. Lenders, and I. Martinovic, "A view from the cockpit: Exploring pilot reactions to attacks on avionic systems," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2020, pp. 1–18.
[29] *Maritime Navigation and Radio Communication Equipment and Systems Class B. Shipborne Equipment of the Automatic Identification System (AIS)—Part 1: Carrier-Sense Time Division Multiple Access (CSTDMA) Techniques*, International Electrotechnical Commission, Geneva, Switzerland, 2017.
[30] *Maritime Navigation and Radiocommunication Equipment and Systems-Class B. Shipborne Equipment of the Automatic Identification System (AIS)—Part 2: Self-Organising Time Division Multiple Access (SOTDMA) Techniques*, International Electrotechnical Commission, Geneva, Switzerland, 2017.
[31] *Maritime Navigation and Radiocommunication Equipment and Systems Automatic Identification Systems (AIS). Part 2: Class a Shipborne Equipment of the Automatic Identification System (AIS) Operational and Performance Requirements, Methods of Test and Required Test Results*, International Electrotechnical Commission, Geneva, Switzerland, 2012.
[32] D. B. Parker, *Toward a New Framework for Information Security*. Hoboken, NJ, USA: Wiley, 2012.
[33] C. Ray, C. Iphar, and A. Napoli, "Methodology for real-time detection of AIS falsification," in *Proc. Maritime Knowl. Discovery Anomaly Detection Workshop*, 2016, pp. 74–77.
[34] W. C. Leite Junior, C. C. de Moraes, C. E. P. de Albuquerque, R. C. S. Machado, and A. O. de Sá, "A triggering mechanism for cyber-attacks in naval sensors and systems," *Sensors*, vol. 21, no. 9, p. 3195, May 2021.
[35] A. Goudossis and S. K. Katsikas, "Towards a secure automatic identification system (AIS)," *J. Mar. Sci. Technol.*, vol. 24, no. 2, pp. 410–423, Jun. 2019.

[36] D. Bothur, G. Zheng, and C. Valli, "A critical analysis of security vulnerabilities and countermeasures in a smart ship system," in *The Proc. 15th Austral. Inf. Secur. Manage. Conf.*, 2017, pp. 81–87.

[37] P. Su, N. Sun, L. Zhu, Y. Li, R. Bi, M. Li, and Z. Zhang, "A privacy-preserving and vessel authentication scheme using automatic identification system," in *Proc. 5th ACM Int. Workshop Secur. Cloud Comput.*, Apr. 2017, pp. 83–90.

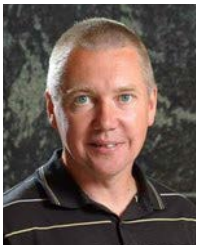
[38] S. Sciancalepore, P. Tedeschi, A. Aziz, and R. Di Pietro, "Auth-AIS: Secure, flexible, and backward-compatible authentication of vessels AIS broadcasts," *IEEE Trans. Depend. Sec. Comput.*, early access, Mar. 30, 2021, doi: 10.1109/TDSC.2021.3069428.

[39] A. Dembovskis, "AIS message extraction from overlapped AIS signals for SAT-AIS applications," Ph.D. dissertation, Dept. Math. Comput. Sci., Univ. Bremen, Bremen, Germany, 2015.

SYED KHANDKER received the M.Sc. degree in web intelligence and service engineering from the University of Jyväskylä, Finland, in 2016, where he is currently pursuing the doctoral degree with the Faculty of Information Technology. Since his childhood, he has been a radio enthusiast and holds an amateur radio operator license. He has authored five journal articles. His research interests include in the field of RF fingerprint positioning, automatic dependent surveillance-broadcast, automatic identification systems, wireless communications, and artificial intelligence.

HANNU TURTIAINEN received the B.Sc. degree in electronics engineering from the University of Applied Sciences, Jyväskylä, Finland, and the M.Sc. degree in cybersecurity from the University of Jyväskylä, Finland, in 2020, where he is currently pursuing the Ph.D. degree in software and communication technology. He is also working in the IoT field as a Cybersecurity and Software Engineer at Binare.io, a deep-tech cybersecurity spin-off from the University of Jyväskylä. His research interests include machine learning and artificial intelligence in the cybersecurity and digital privacy field.

ANDREI COSTIN received the Ph.D. degree from EURECOM/Télécom ParisTech, in 2015, under co-supervision of Prof. Francilon and Prof. Balzarotti. He is currently a/an Senior Lecturer/Assistant Professor in cybersecurity with the University of Jyväskylä, Central Finland, with a particular focus on the IoT/firmware cybersecurity and digital privacy. He has been publishing and presenting at more than 45 top international cybersecurity venues, both academic (Usenix Security and ACM ASIACCS) and industrial (BalckHat, CCC, and HackInTheBox). He is the author of the first practical ADS-B attacks (BlackHat 2012) and has literally established the large-scale automated firmware analysis research areas (Usenix Security 2014)—these two works are considered seminal in their respective areas—being also most cited at the same time. He is also the CEO/Co-Founder of Binare.io, a deep-tech cybersecurity spin-off from the University of Jyväskylä, focused on innovation and tech-transfer related to the IoT cybersecurity.



TIMO HÄMÄLÄINEN has over 25 years of research and teaching experience related to computer networks. He has lead tens of external funded networks management related projects. He has launched and leads master's programs in the University of Jyväskylä (currently SW and Comm. Eng.) and teaches networks management related courses. He has more than 200 internationally peer-reviewed publications, and he has supervised 36 Ph.D. theses. His current research interests include wireless/wired networks resource management (the IoT, SDN, and NFV) and networks security.