Dude, Where's That Ship? Stealthy Radio Attacks Against AIS Broadcasts

Felix Klör[•°], Jan Bauer[•], Sachar Paulus[*], and Michael Rademacher[•°]

[•]Fraunhofer FKIE
Cyber Analysis & Defense
Wachtberg, Germany

[°]Hochschule Bonn-Rhein-Sieg
Department of Computer Science
Sankt Augustin, Germany

[*]Mannheim University of Applied Sciences
Faculty of Computer Science
Mannheim, Germany

{<firstname>.<lastname>}@fkie.fraunhofer.de

s.paulus@hs-mannheim.de

***Abstract*—The Maritime Transportation System (MTS) is the foundation of global trade, a crucial pillar of our economy's supply chains, but also critical to energy and food security. At the same time, it is increasingly exposed to new types of threats. These include attacks from the cyber and electromagnetic spectrum against various information and telecommunications systems on board vessels as the backbone of the MTS. The radio-based Automatic Identification System (AIS) is one of these systems, used to monitor ship routes and for traffic planning, and supports collision avoidance on the vessel side. The technical vulnerabilities of the system have long been known and caution is therefore advised. Conventional attacks are usually easy to recognize, so that disruptions to operations can occur, but serious damage can be limited. In this paper, however, we present a novel radio-based attack on AIS that enables to selectively suppress identification messages of individual ships and thus to manipulate the situational awareness on the vessel's bridge in a *stealthy* manner, which can have catastrophic impacts in critical situations. We demonstrate the technical feasibility of this attack in a laboratory environment with real hardware and, by elaborating this vulnerability, we are contributing to increasing the resilience of the maritime domain against evolving hybrid threats.**

***Index Terms*—Automatic Identification System; Electronic Warfare; Selective Jamming; Maritime Cyber Security; Integrated Bridge System**

I. Introduction

The majority of the world's traded goods and resources are shipped by sea through a complex global Maritime Transportation System (MTS) that forms the backbone of global trade. It thus plays a pivotal role in today's production and supply chains and ensures energy and food security at a global scale. However, the obstruction of the Suez Canal by the *Ever Given* in 2021 [1], the Russian blockade of Ukrainian grain exports in the Black Sea in 2022 [2], and the recent attacks on merchant ships off the Yemeni coast by the Houthi militia [3] are just a few examples that remind us how fragile our MTS is and how huge the impact of disruptions can be.

In addition to these human and geopolitical influences on the security of the MTS, it is increasingly confronted with new threats from cyberspace due to growing digitalization, the ever-increasing level of automation, and the pervasive networking and interconnection of globally distributed systems [4]–[7]. Moreover, there are threats from the electromagnetic spectrum that target communication and navigation technologies as well as cyber-physical sensor systems [8].

Maritime stakeholders are already aware of the high risk to the MTS, arising from both the cyber domain and electromagnetic spectrums. Besides ports and other maritime infrastructures, their focus is particularly on vessels as an elementary component of the MTS. With resolution MSC.428(98) [9], the International Maritime Organization (IMO) has urged shipping companies to address cyber risks in their safety management systems from 2021 at the latest. The Baltic and International Maritime Council (BIMCO) and the classification society DNV, for instance, also have extensive requirements regarding the cyber security of maritime systems on board ships, some of which also include protection against electromagnetic attacks [10, 11].

Recently, the International Association of Classification Societies (IACS) published unified security requirements that will become mandatory for the classification of new ships from July 2024 [12, 13], thus making a first step towards mandatory cyber security. These requirements address all IT, Operation Technology (OT), and communication systems on board, in particular the equipment of the integrated bridge system, above all the Electronic Chart Display and Information System (ECDIS), the radar, and also the Automatic Identification System (AIS).

The AIS represents an essential radio-based communication infrastructure within the maritime domain [14, 15] and, according to the SOLAS convention [16], is mandatory for most commercial vessels on international voyages. It facilitates real-time data exchange among vessels and also between shore-based stations and aids to navigation (AtoNs), cf. Fig. 1, enabling automated transmission of unique identification, crucial navigational parameters including Hence, AIS is nowadays used for Vessel Traffic Service (VTS), monitoring, and long-range tracking, for route planning and orchestration in fleet operation centers (FOCs), search and rescue operations, but also in the context of anomaly detection by authorities, organizations, and academia [17, 18].

While vessels primarily utilize AIS to convey their navigational status, this information is not only accessible on AIS devices but can also be firmly integrated into other bridge components, e.g., ECDISs and radar terminals. In this way, the dissemination of AIS messages significantly enhances navigational efficacy and situational awareness, enabling early detection of potential hazards and collisions. Particularly in crowded maritime scenarios or during periods of limited visibility, AIS emerges as an indispensable tool for safe navigation.

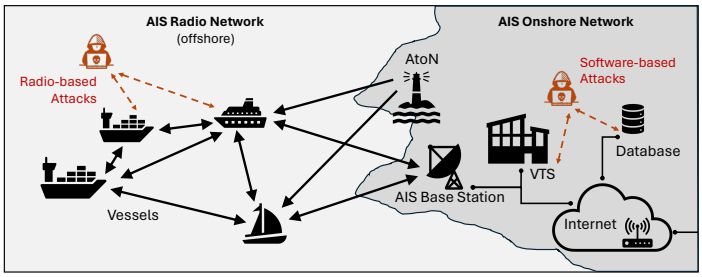


Fig. 1. Overview of the maritime AIS broadcast between vessels at sea and coastal infrastructures, as well as possible categories of attacks (highlighted in red and discussed later in Section II-C).

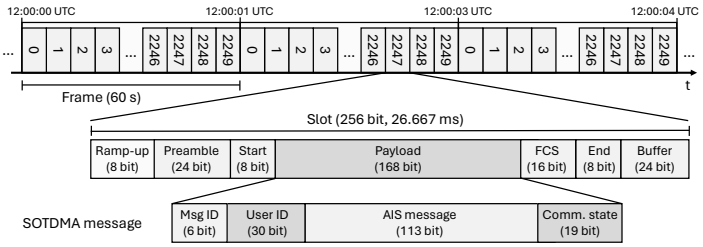


Fig. 2. AIS TDMA frame and message format as specified by the ITU-R [15].

From a security perspective, the ubiquitous relevance of AIS for the shipping industry necessitates the assurance of its integrity and authenticity, but above all the reliability and the availability of this service to be ensured. However, research has identified serious security risks with AIS in the last decade. These risks range from AIS spoofing via implementation-specific data poisoning of online databases [19] to protocol-specific radio attacks against transponders, such as denial of service (DoS), spoofing, or hijacking attacks, for all of which there is numerous evidence of incidents in the real world [17, 19, 20].

The vulnerability of AIS to malicious activities emphasizes the imperative to strengthen its resilience, as any compromise could pose significant risks to both the aforementioned MTS and human lives. In light of these considerations, this paper investigates a novel radio-based attack vector targeting the AIS. By proactively introducing this security vulnerability, we aim to mitigate potential hybrid threats at their inception, thereby safeguarding the reliability of this indispensable maritime communication system. The contributions of our work include:

- introduction of a new AIS vulnerability related to covert, selective jamming with the resulting threat model, and
- the prototypical realization of a novel AIS attack using a commercial off-the-shelf Software Defined Radio (SDR) and its real-world evaluation in a laboratory environment.

The remainder of the paper is organized as follows. After introducing the technical background on AIS and reviewing the known security threats and related work in Section II, we present the identified attack vector and the corresponding threat model (Section III). Then, in Section IV, the concept and the prototypical implementation of our new radio attack are explained, and how it exploits the AIS design. This implementation is subsequently evaluated in a laboratory environment (Section V). After discussing the results of our prototype, Section VI finally concludes the paper.

II. Technical Background

This section provides the technical background required for this work. First, a brief overview of AIS is given (Section II-A). Section II-B then offers a more detailed insight into the self-organized media access, which is of particular importance for the implementation of the novel attack. We close this section with a discussion of known vulnerabilities and related work in the field of AIS security in Section II-C.

A. Automatic Identification System in a Nutshell

In the Automatic Identification System, messages are exchanged by transceivers, so-called AIS stations, and include e.g., the vessel's call sign, its Maritime Mobile Service Identity (MMSI), as well as nautical course and voyage-related information [15]. While there are different types of stations depending on the deployment location and purpose, we focus on Class A mobile ship-borne stations in this paper since all ships of IMO member states exceeding an internal volume of 300 GT or are classified as a certain ship type (e.g., as passenger ferry) require such stations [16]. Hence, the majority of vessels in commercial shipping worldwide are equipped with them.

Each Class A station is provided with a Global Navigation Satellite System (GNSS) and a very high frequency (VHF) antenna. Depending on the antenna height, the range of ship-to-ship transmissions is typically 20 nm (≈37 km), whereas coastal stations receive signals within hundreds of kilometers [18]. GNSS is used for Positioning, Navigation, and Timing (PNT), while the actual AIS messages are received and transmitted via the VHF Data Link (VDL). Nowadays, AIS stations not only offer their own user interface (UI) but are also highly networked with other onboard systems within the Integrated Bridge System (IBS) allowing to include dynamic course information into transmitted messages, such as position, heading, speed, or rate of turn and, vice versa, the integration of received AIS signals into radar and chart displays.

At the physical layer, two VHF channels at 161.975 MHz and 162.025 MHz are used, on which the transmission alternates, each with a bandwidth of 25 kHz and a nominal data rate of 9600 bits/s [15]. The actual data bits are non-return-to-zero inverted (NRZI) encoded and then modulated onto the carrier signal using Gaussian Minimum Shift Keying (GMSK).

The link layer controls access to the VHF channels using Time Division Multiple Access (TDMA) techniques and defines frame and message formats. A frame has a duration of 1 min and is synchronized by the UTC time. It is divided into 2250 individual transmission slots per channel. Each slot provides a station with a transmission time of 26.667 ms and 256 bit [15], cf. Fig. 2. Time synchronization can be done directly via PNT or, if not available, indirectly through messages received.

The message format, outlined in Fig. 2 as well, begins with an 8-bit ramp-up phase along with a 24-bit preamble. Following the High-Level Data Link Control (HDLC) protocol, the actual AIS payload (168 bit) is enclosed to 8-bit start and end flags and protected by the subsequent Frame Check Sequence (FCS)

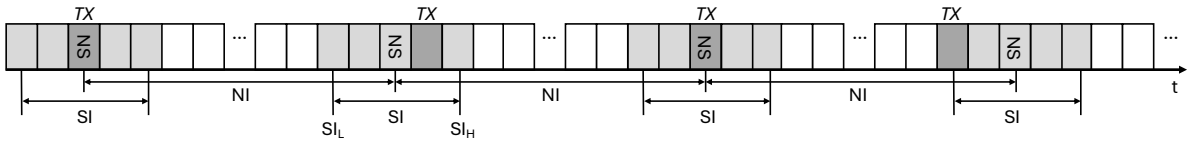


Fig. 3. Randomized slot map access scheme using AIS's Self-Organized TDMA (SOTDMA) (simplified example according to [15]).

field, i.e., a 16-bit Cyclic Redundancy Check (CRC). Finally, a 24-bit buffer compensates for excess bits due to bit stuffing and for the impact of transmission delays, e.g., caused by the distance or jitter of the stations.

In total, there are 27 message types currently defined in the standard [15], of which the position report (message ID 1-3) is the most frequent type for Class A stations. Its transmission frequency depends on the vessels' maneuvers, i.e., the sending interval decreases with increasing speed in the range from 3 min (anchored or moored) up to 2 s (>23 knots) [15].

B. AIS's Self-Organized TDMA

In the main operating mode of a vessel's Class A station, the continuous operation phase, the so-called Self-Organized TDMA (SOTDMA) is used for assigning slots without a central entity. For this purpose, the fixed message transmission interval, called nominal reporting interval (NI), defines periodic nominal slots (NSs). However, they only serve as an initial starting point for the station's actual transmission slot *TX*, as shown in Fig. 3. Based on that starting point, *TX* is then randomly placed with a slight variation in a discrete selection interval (SI) defined by:

$$TX \in \mathrm{SI} \coloneqq [\mathrm{SI}_L, \mathrm{SI}_H] = [\mathrm{NS} - 0.1 \times \mathrm{NI}, \mathrm{NS} + 0.1 \times \mathrm{NI}].$$

In addition, all selected transmission slots of a frame are only reused for a certain duration in subsequent frames. For this purpose, each *TX* is assigned a 3-bit integer *timeout* counter, which is also always randomly initiated ($\in$[3,7]). After each transmission, this timeout is decremented and, if expires, it is reset and a new slot must be determined.

Hence, SOTDMA transmission slots are not fully deterministic. The randomization serves to avoid transmission collisions in this decentralized media access procedure. However, for better coordination, stations proactively announce the change of each slot in their messages. For this purpose, there is a communication state field at the end of the SOTDMA message, while a User ID contains the MMSI of the sending vessel, cf. Fig. 2. The communication state includes, among other things, the transmission *timeout* and alternately the number of stations received or the current slot number for the sake of synchronization, cf. [15]. To announce the upcoming slot change, the communication state finally contains a *slot offset* in case the timeout value is 0, providing the number of slots between the current and the new slot in the following frame.

C. AIS Vulnerabilities

The AIS standard, which dates back to the 2000s, is designed for flawless global operation and aims for functional safety, reliability, and decentralization in the exchange of navigation and other ship data. However, it does not address information security and AIS broadcasted messages are neither encrypted nor authenticated [21, 22].

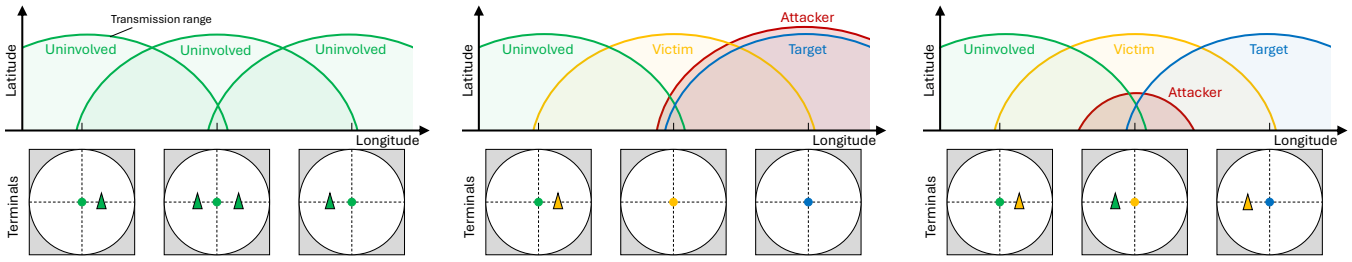
Serious vulnerabilities have thus been identified already a decade ago by Balduzzi *et al.* [19], who differentiate between *software-based attacks* against the onshore AIS information system, such as data poising [23] as happened recently with NATO warships that appeared near the Russian-occupied territory of Ukraine [24, 25], and *radio-based attacks*, which comprise spoofing, hijacking, and disruptions of availability attacks, cf. Fig. 1. The former radio attacks either craft legitimate AIS messages impersonating IDs of their victims or alter ongoing transmissions by overpowering the original radio signal with a manipulated one. The latter, in contrast, can be executed in three different ways, i.e., slot starvation, frequency hopping, or timing attacks, by attackers pretending to be a maritime authority leveraging control messages to influence nearby stations.

Based on Balduzzi's pioneering work, Kessler *et al.* [20] present a more detailed classification including an estimation of likelihood, impact, and ease for each attack type, while Levy *et al.* [17] surveys further possible attacks, e.g., fuzz and penetration testing as well as binary message injection into the IBS, similar to the bridge attack tool [7]. Finally, others *et al.* [26, 27] investigate how AIS can be misused to trigger malware implanted in IBSs, whereas Soner *et al.* [28] conduct a human risk assessment regarding the AIS.

The practical feasibility of radio-based AIS attacks, with which it would be possible to create e.g., non-existing vessels that are on collision, has also already been shown by Balduzzi *et al.* [19] in a laboratory environment and confirmed by further demonstrations [29]–[31]. In this context, often SDRs and the GNU Radio [32] software AISTX are used [19, 30, 31], but inexpensive single-board computers are also suitable for such attacks, such as Raspberry Pis [30]. Khandker *et al.* moreover discussed AIS disruptions using radio jamming and experimentally demonstrate the total interruption of AIS reception during continuous jamming. As they do not yet address the jamming of individual messages using protocol-aware reactive or selective jamming approaches known from other domains, e.g., [33, 34], their jamming attack is not complex to detect and, therefore, has a disruptive rather than threatening character.

III. New Attack Vector

Based on the existing vulnerabilities of the AIS and the related work discussed, we now present a novel radio-based attack vector, to which the shipping industry and the MTS are neither immune nor fully prepared. We will first introduce the basic idea and goals of this attack (Section III-A) and then address our assumptions in our threat model (Section III-B).



(a) Benign scenario. (b) Conventional AIS jamming. (c) Selective AIS jamming (our approach).

Fig. 4. Functionality of the new selective jamming attack in a simplified three-ship scenario (a) assuming omnidirectional antennas. Instead of jamming loudly and obviously (b), it silently and stealthily removes the selected target from the victim's screen without affecting the reception of uninvolved stations (c).

A. Attack Goals

Instead of carrying out a noticeable, tangible attack against the operational services to disrupt or paralyze shipping traffic, as in many availability disruption attacks [19, 31], our new type of radio attack is designed to remain as undetected as possible and, thus, lead to navigation failures with serious harm. Thus, it aims to selectively attack only individual AIS stations, referred to as *targets*, rather than all stations in the transmission range.

Note that the forged AIS control commands mentioned in the previous section, such as slot starvation [19], can also be used selectively. However, they require a certain spatial proximity to the target, since they require a bidirectional radio link. Our approach is therefore intended to directly attack the receiving station of those targets, which is the actual *victim*. For this purpose, it is based on carefully coordinated and time-limited jamming pulses that are precisely aimed at interfering with the reception of AIS messages of individual *target* vessels, respectively their Class-A AIS stations. This selective cancellation could impact the decisions of a navigator. In critical situations, such as in narrow and busy passages and in poor visibility, and executed at the right time, the new selective jamming attack could thus provoke devastating wrong navigational decisions of the victim and ultimately even lead to collisions and groundings.

In contrast to conventional attacks that are based on extensive and continuous jamming, our approach does not cause an obvious (total) disruption but is selective and, thus, difficult to detect on the screen of an operator. Moreover, due to its targeted and very short jamming pulses, it is particularly stealthy. Compared to attacks leveraging forged control commands, our approach could not be prevented by cryptographic countermeasures introduced in the literature, e.g., [14, 21, 22, 35], since it does solely depend on AIS's media access procedure.

B. Threat Model

In our threat model, we assume an *attacker* with moderate skills but with AIS-specific knowledge and a high motivation to cause targeted damage. They only need low resources, i.e., generally available low-cost hardware. Moreover, we assume the *attacker* to be in spatial proximity (i.e., in radio interference range) to its *victim* and only in reception range of the target.

An abstract scenario with three vessels is shown in Fig. 4, which outlines the functionality of the novel attack. In the benign case (Fig. 4(a)), the middle vessel receives the AIS messages from the two neighboring vessels, which are not in the transmission range of each other. Conventional jamming superimposes the original signal of the *target* with high transmission power and prevents it from being received by the *victim*, cf. Fig. 4(b). However, this jamming is "loud" and can therefore be easily detected and localized using Electronic Signals Intelligence (ELINT). It also prevents the target from receiving AIS messages. With the selective jamming (Fig. 4(c)), presented in this work, the *attacker* can significantly reduce the transmission power if they are in close proximity to the *victim* and thus, in combination with a short duration that is limited to the target's transmission slots, can operate stealthily.

The proximity to the victim could be realized via air- or water-borne unmanned vehicles, e.g., low-cost drones, but also less sophisticated by means of directional radio antennas from the coast, e.g., in busy straits or canals. The pre-deployoment of the jammer hardware on a vessel is also possible. A remote connection is then required for situational control of the attack, but also automation of the attack would be conceivable, which could be enabled by a position-triggered algorithm that removes possible AIS signals on a collision course.

IV. Concept & Implementation

Our concept aims to precisely jam every AIS message of a selected target. The fundamental challenge here is that it is necessary for the attacker to know the current transmission slots of the target and to be aware of announced changes in order to continue properly in subsequent frames (cf. Sec. II-B). Consequently, the jamming of the selected messages must not be too extensive, because the announcements must still be received by the attacker itself. Thus, we rely on short jamming pulses, which only jam a message as little as possible and at irrelevant sections, but still cause a CRC failure, resulting in the message being discarded by a regular transceiver. According to the designed architecture and as visualized by the flow graph in Fig. 5, the attacker can be logically divided into three modules, i.e., the receiver, a scheduler, and the actual jammer, which are described in the following subsections.

A. Receiver

The receiver module handles the digital signal processing of the AIS messages on both channels simultaneously. First,

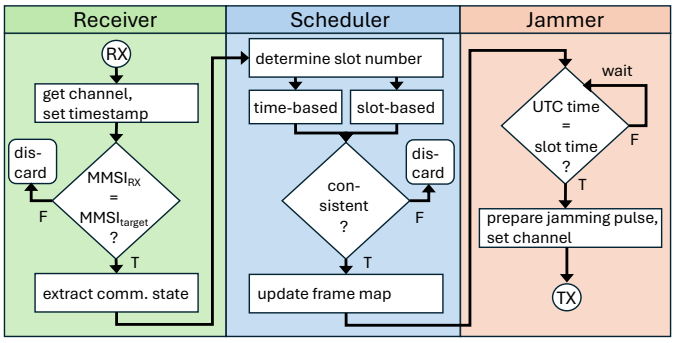


Fig. 5. Simplified message processing of the implemented selective jammer.

the incoming signals are filtered through a low-pass filter and stabilized to a constant gain level. This is followed by a clock recovery with subsequent GMSK demodulation. The result is a continuous bit stream containing the desired information.

To be able to also receive jammed messages, we modified the regular reception method. First, we filter messages in the incoming bitstream for the selected target User ID (i.e., MMSI) and check the validity of start and end flags. Then, we extract the communication state, i.e., the last 24 bit due to potential bit stuffing of this 19 bit message field (cf. Fig. 2), and forward it to the scheduler together with a timestamp.

B. Scheduler

The scheduler module has the task of managing a frame map for the target in which, at any point in time, the current and future transmission slots of the target are maintained. Therefore, it first decodes the received communication state and checks its validity. Then, it determines the slot of the message from which the communication state was extracted. On the one hand, the recorded timestamp is used for this, as, when synchronized, the slot number can be calculated from the time of receiption (cf. Sec. II). On the other hand, the slot number occasionally contained in the communication state is also used directly and this is updated with the offset announced for slot changes. Both methods, time-based and slot-based, are then checked for consistency. In the event of inconsistencies, only warnings are issued in our prototype implementation. Intelligent error handling is not necessary for our evaluation with ideal synchronization and remains as future work. The determined slots are then transferred with the corresponding channel from which the message originates to the aforementioned frame map, which is permanently updated in this way and also shared with the jamming module.

C. Jammer

The jamming module calculates the next transmission slot of the target from the current UTC time and the slot number. A corresponding offset is added so that the preamble and the User ID are not affected. Finally, a short jamming pulse is sent on the frequency of the corresponding channel as soon as the calculated time is reached. A fixed, 1.9 ms long section of an arbitrarily recorded AIS message is used as the interference signal. As a result, the message of the target is

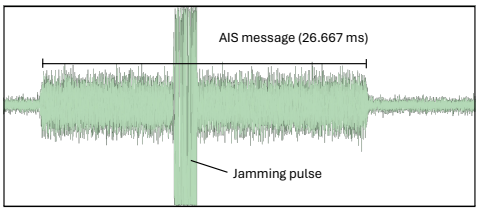


Fig. 6. AIS message (position report, ID 1, SOTDMA) jammed by a short jamming pulse that slightly overpowers the original signal and precisely hits the message between the User ID and the communication state, cf. Fig. 2.

disrupted precisely and effectively during transmission, but without destroying information relevant to the attacker, as the image of an example jamming in Fig. 6 illustrates.

V. Evaluation

For regulatory reasons, it is not possible for us to test the developed selective AIS jammer in the wild. Therefore, we use a protected laboratory environment to evaluate our prototype, in which we can safely transmit and jam the AIS with limited transmission power. In addition, signals from real vessels that were previously recorded outdoors are used for a practical evaluation. Our experimental setup is described in Section V-A. The experiments and results are then discussed in Section V-B.

A. Experimental Setup

The evaluation setup, depicted in Fig. 7, is based on experimental SDRs and comprises three components: the AIS *replayer*, the developed *jammer*, and the *victim* station. For the former, Universal Software Radio Peripheral (USRP) B210 SDRs with GNU Radio are used, similar to [19, 30, 31] (cf. Section II-C). For the sake of modularity, the *jammer* consists of two devices and thus handles receiving and jamming separately. In contrast, the *victim* is deliberately implemented using unmodified commercial off-the-shelf hardware, i.e., a Raspberry Pi with the low-cost dAISy-HAT. Finally, strict time synchronization for TDMA is provided by an OctoClock module, which supplies all SDRs with a pulse per second (PPS) signal derived from GNSS and a 10 MHz reference signal.

In the experiments, the *replayer* plays back the AIS tracks (I/Q samples) recorded on the Rhine, collected with a B210 (162 MHz center frequency, 76 dB gain) on an elevated

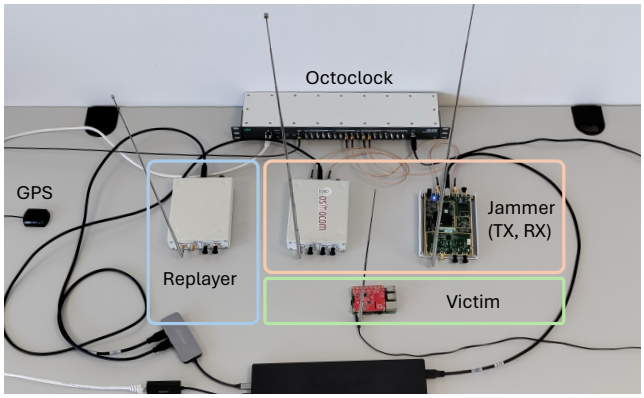


Fig. 7. Experimental laboratory setup to validate the selective jamming attack.

TABLE I
INFORMATION AND KEY NUMBERS ON THE RECORDED AIS DATA.

Location:	Rhine, Drachenfels platform, Germany			
PNT:	N 50°39′51.7″ E 7°12′35.6″, 04/18/2024			
Duration [min]:	21.5		Size [GB]:	10.32
# vessels:	30		# AIS msg.:	2178
AIS type (#):	1 (1806)	3 (243)	5 (56)	8 (59)

platform (≈220 m above the river) with good line-of-sight conditions allowing for AIS reception with a distance of up to 20 km. Statistics on this recordings can be found in Tab. I and a track visualization of two exemplary vessels in Fig. 8 (right). Note that replaying is trivial as AIS messages do not contain absolute date/time information.

B. Experiments & Results

To demonstrate the general practical feasibility of our approach, but also to quantitatively investigate the effectiveness of the developed selective jammer, two series of tests were carried out with the laboratory setup. First, the recorded AIS track was transferred as a baseline for our evaluation without the influence of the jammer (*benign*). Then, the jammer was activated during the entire next run (*jamming*). Both test series were repeated alternately four times to mitigate the potential influence of external interference factors on the radio transmission.

From all 30 vessels of the recorded track, a vessel was selected that had been in the reception radius for a sufficiently long time during the measurement and had average, representative characteristics. This is the *RP Bern* (MMSI 269057006), a typical tanker for the Rhine. Note that the ship with the most frequent messages (MMSI 211697470) is a local passenger ferry shuttling between the two riversides, cf. Fig. 8 (right).

The results of our experiments are visualized in Fig. 8 (left) showing the number of AIS messages received by the receiver/victim per vessel (MMSI) as a barplot. Vessels with few transmissions are excluded here. The green bars represent the averaged results in the benign scenario and the blue ones during selective jamming. A slight but nevertheless existing variance can be seen in both series, which can be explained by natural interference and was increased by the reduced transmission power. Overall, however, it can be seen that the series are stable.

The interesting part is obviously the comparison of both test series (green vs. blue bars). It is evident that the developed jammer effectively jams the transmissions of the selected target, while the reception of the other transmissions from non-targets remains virtually unaffected. Only for some of the vessels are the blue bars slightly smaller than the green bars. It is unlikely that this is due to the collateral effects of the jammer, as the short jamming pulses were applied very precisely. An analysis gave no indication of a possible temporal overshooting.

However, the comparison of the two bars of the target in Fig. 8 also clearly shows that not all of the target's messages were jammed. Instead, a constant number of 6 messages can be received at the victim for all replications. The reason for this lies in the nature of the developed jammer, which must first gain knowledge of the target's slot map by receiving AIS messages

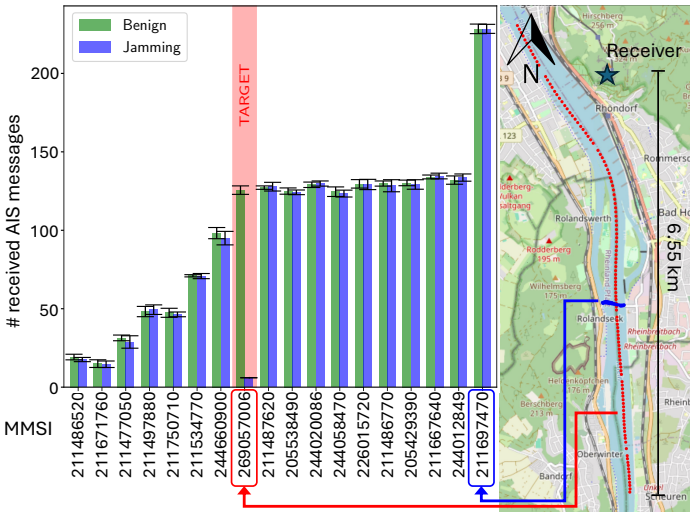


Fig. 8. The experimental comparison of benign experiments (w/o jamming) with the selectively jammed series proves that our approach actually enables the jamming of only the messages of an arbitrarily selected target, while the remaining radio transmissions of other vessels remain unaffected. Note that real pre-recorded AIS data serves as the basis for this experiment, exemplarily depicted on the right. MMSI-to-vessel resolution is provided e.g., by [36].

from the target, cf. Sec. IV. Because at the speed at which vessels travel on the Rhine, the position reports (type 1) are broadcast every 10 s, i.e., 6 messages per frame. After receiving all of these 6 messages once, the jammer has learned the slot allocation. Our evaluation results reveal that the jammer then immediately operates successfully with a total hit rate.

C. Discussion & Limitations

The results achieved by our approach in the laboratory must, of course, be be assessed in relation. A laboratory has inherent limitations, as transmission power and communication distances of the real world cannot be reproduced identically. Furthermore, our experiments are based on SDRs and low-cost hardware. No professional devices were used. In addition, the time was synchronized between all transceivers via a shared PPS signal and the impact of possible jitter on jamming capabilities has not yet been investigated. Finally, in future work, we will also analyze the effect of interrogation, i.e. the requesting of reports, and, if necessary, extend our approach so that explicit polling of the target still remains unanswered.

VI. CONCLUSION

In this paper, we presented a novel radio attack against the global maritime Automatic Identification System (AIS), whose detection is hardly possible for the navigator due to its stealthy behavior. Used in the right situation, this attack can thus have a dramatic impact. It exploits the predictability of the transmission slots to selectively disrupt the transmissions of a chosen target with short jamming pulses. Based on realistic experiments using commercially available SDRs, we demonstrated the feasibility of such an attack in a laboratory environment to raise awareness of the serious threat that cannot be prevented with the current AIS. However, detection, e.g., based on observed erroneous transmissions, may be possible, which we will investigate in our future work.

References

[1] J. M.-Y. Lee and E. Y.-C. Wong, "Suez Canal blockage: an analysis of legal impact, risks and liabilities to the global supply chain," in *MATEC Web of Conferences*, vol. 339, 2021.

[2] Council of the EU and the European Council, "Ukrainian grain exports explained," 2024. [Online]. Available: https://www.consilium.europa.eu/en/infographics/ukrainian-grain-exports-explained/

[3] S. Scarr, A. Arranz, J. Saul, H. Huang, J. Chowdhury, and V. M. Kawoosa, "Red Sea attacks," 2024. [Online]. Available: https://www.reuters.com/graphics/ISRAEL-PALESTINIANS/SHIPPING-ARMS/lgvdnngeyvo/

[4] B. Svilicic, J. Kamahara, M. Rooks, and Y. Yano, "Maritime Cyber Risk Management: An Experimental Ship Assessment," *Journal of Navigation*, vol. 72, no. 5, pp. 1108–1120, 2019.

[5] M. Caprolu, R. D. Pietro, S. Raponi, S. Sciancalepore, and P. Tedeschi, "Vessels Cybersecurity: Issues, Challenges, and the Road Ahead," *IEEE Communications Magazine*, vol. 58, no. 6, Jun. 2020.

[6] V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos, "A novel cyber-risk assessment method for ship systems," *Safety Science*, vol. 131, pp. 14, art. no. 104 908, 2020.

[7] C. Hemminghaus, J. Bauer, and E. Padilla, "BRAT: A BRidge Attack Tool for Cyber Security Assessments of Maritime Systems," *Int. Journal on Marine Navigation and Safety of Sea Transportation (TransNav)*, vol. 15, no. 1, 2021.

[8] A. Amro, V. Gkioulos, and S. Katsikas, "Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework," *ACM Transactions on Privacy and Security*, vol. 26, no. 2, 2023.

[9] IMO MSC.428(98), "Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems," International Maritime Organization (IMO), June 2017.

[10] BIMCO, "The Guidelines on Cyber Security Onbaord Ships (Version 4)," The Baltic and International Maritime Council (BIMCO), 2020.

[11] IEC 62443-4-2, "Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components," 2019.

[12] IACS, "UR-E26 – Cyber resilience of ships," International Association of Classification Societies (IACS), Unified Requirements, Apr. 2022.

[13] ——, "UR-E27 – Cyber resilience of on-board systems and equipment," International Association of Classification Societies (IACS), Unified Requirements, Apr. 2022.

[14] S. Sciancalepore, P. Tedeschi, A. Aziz, and R. D. Pietro, "Auth-AIS: Secure, Flexible, and Backward-Compatible Authentication of Vessels AIS Broadcasts," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 04, pp. 2709–2726, 2022.

[15] ITU, "Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band," International Telecommunication Union (ITU), Recommendation ITU-R M.1371-5 (02/2014), M Series – Mobile, radiodetermination, amateur and related satellite services, 2014.

[16] IMO SOLAS, "SOLAS Chapter V – 1/7/02, Safety of Navigation," International Maritime Organization (IMO), 2020.

[17] S. Levy, E. Gudes, and D. Hendler, "A Survey of Security Challenges in Automatic Identification System (AIS) Protocol," in *Proc. of the Int. Symposium on Cyber Security, Cryptology, and Machine Learning (CSCML)*, Be'er Sheva, Israel, 2023, pp. 411–423.

[18] K. Wolsing, L. Roepert, J. Bauer, and K. Wehrle, "Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches," *Journal of Marine Science and Engineering*, vol. 10, no. 1, 2022.

[19] M. Balduzzi, A. Pasta, and K. Wilhoit, "A Security Evaluation of AIS Automated Identification System," in *Proc. of the 30th Annual Computer Security Applications Conference (ACSAC)*, New Orleans, LA, USA, 2014, pp. 436–445.

[20] G. C. Kessler, J. P. Craiger, and J. C. Haass, "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System," *Int. Journal on Marine Navigation and Safety of Sea Transportation (TransNav)*, vol. 12, no. 3, 2018.

[21] A. Aziz, P. Tedeschi, S. Sciancalepore, and R. D. Pietro, "SecureAIS - Securing Pairwise Vessels Communications," in *Proc. of the Conference on Communications and Network Security (CNS)*, Avignon, France, 2020, pp. 1–9.

[22] A. Goudosis and S. Katsikas, "Secure AIS with Identity-Based Authentication and Encryption," *Int. Journal on Marine Navigation and Safety of Sea Transportation (TransNav)*, vol. 14, no. 2, pp. 287–298, 2020.

[23] I. Botunac and M. Gržan, "Analysis of Software Threats to the Automatic Identification System," *Brodogradnja*, vol. 68, no. 1, pp. 97–105, 2017.

[24] H. I. Sutton, "Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base," 2021, USNI News. [Online]. Available: https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base

[25] G. C. Kessler and D. M. Zorri, "AIS Spoofing: A Tutorial for Researchers," in *Proc. of the 2nd LCN Special Track on Maritime Communication and Security (MarCaS)*, Caen, France, 2024.

[26] 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, 2021.

[27] A. Amro and V. Gkioulos, "From Click to Sink: Utilizing AIS for Command and Control in Maritime Cyber Attacks," in *Proc. of the 27th European Symposium on Research in Computer Security (ESORICS)*, Copenhagen, Denmark, 2022, pp. 535–553.

[28] O. Soner, G. Kayisoglu, P. Bolat, and K. Tam, "Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks," *Applied Ocean Research*, vol. 142, pp. 14, art. no. 103 855, 2024.

[29] M. M. Marques, D. Teles, V. Lobo, and G. Capela, "Low-cost AIS Transponder using an SDR device," in *Proc. of OCEANS 2019 MTS/IEEE*, Seatle, WA, USA, 2019, pp. 1–4.

[30] D. Barber, V. Kanth, and D. Rogers, "Manipulating the Automatic Identification System with Extremely Low-Cost Hardware," in *Proc. of the Military Communications Conference (MILCOM)*, Rockville, MD, USA, 2022, pp. 541–546.

[31] S. Khandker, H. Turtiainen, A. Costin, and T. Hämäläinen, "Cybersecurity Attacks on Software Logic and Error Handling Within AIS Implementations: A Systematic Testing of Resilience," *IEEE Access*, vol. 10, pp. 29 493–29 505, 2022.

[32] GNU Radio project, "The Free & Open Software Radio Ecosystem," 2024. [Online]. Available: https://www.gnuradio.org/

[33] D. Nguyen, C. Sahin, B. Shishkin, N. Kandasamy, and K. R. Dandekar, "A real-time and protocol-aware reactive jamming framework built on software-defined radios," in *Proc. of the ACM Workshop on Software Radio Implementation Forum (SRIF)*, Chicago, Illinois, USA, 2014, pp. 15–22.

[34] E. Aras, N. Small, G. S. Ramachandran, S. Delbruel, W. Joosen, and D. Hughes, "Selective Jamming of LoRaWAN using Commodity Hardware," in *Proc. of the 14th EAI Int. Conf. on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous)*, Melbourne, Australia, 2017, pp. 363–372.

[35] G. C. Kessler, "Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity," *Int. Journal on Marine Navigation and Safety of Sea Transportation (TransNav)*, vol. 14, no. 2, 2020.

[36] VesselFinder, "Vessels database – ais ship positions," 2024. [Online]. Available: https://www.vesselfinder.com/vessels