engineering proceedings

MDPI

Proceeding Paper

The Vulnerability of Inland Waterway AIS to GNSS Radio Frequency Interference †

Jakub Steiner [1,2,*], Jakub Havlíček [1], Tomáš Duša [1] and Günter Heinrichs [3]

[1] GNSS Centre of Excellence, 14200 Prague, Czech Republic
[2] Department of Air Transport, Faculty of Transportation Sciences, Czech Technical University in Prague, 12800 Prague, Czech Republic
[3] Spirent Communications, Crawley RH10 1BD, UK; guenter.heinrichs@spirent.com
* Correspondence: steinja8@fd.cvut.cz
† Presented at the European Navigation Conference 2023, Noordwijk, The Netherlands, 31 May–2 June 2023.

Abstract: GNSS is an indispensable source of positioning, navigation and timing for many sectors, including inland waterway transport. Unfortunately, GNSS is also vulnerable to interference, including intentional jamming and spoofing. This paper evaluates the vulnerability of one of the key inland waterway systems—the automatic identification system (AIS)—to GNSS jamming and spoofing. The vulnerability is explored via a series of tests conducted in both laboratory and live-sky environments. The results clearly show the negative impact of both types of interference on AIS. The impact included denial of service and reporting of false position. Additionally, the effects on subsequent systems like river information services or nearby vessels are also showcased. The results presented provide valuable insight into the vulnerability of inland waterway transport. The need for understanding the system limitations and vulnerability rises with the increase in the implementation of autonomous systems into the inland waterway sector, as well as other critical infrastructure sectors.

Keywords: GNSS; GPS; interference; jamming; spoofing; automatic identification system (AIS); vulnerability; inland waterways; critical infrastructure

Citation: Steiner, J.; Havlíček, J.; Duša, T.; Heinrichs, G. The Vulnerability of Inland Waterway AIS to GNSS Radio Frequency Interference. *Eng. Proc.* **2023**, *54*, 26. https://doi.org/10.3390/ENC2023-15461

Academic Editors: Tom Willems and Okko Bleeker

Published: 29 October 2023

1. Introduction

Over the past decades, Global Navigation Satellite Systems (GNSS) have become an indispensable utility for many sectors of critical infrastructure (CI) as a reliable and accurate source of positioning, navigation and timing (PNT) [1]. In the CI sector of inland waterway transport, GNSS is predominantly used for vessel position determination and vessel tracking where GNSS is the primary and often the sole PNT source [1,2].

The specific system used by inland vessels for position determination is called the inland automatic identification system (AIS). The AIS also broadcasts the vessel's position and its identification, course, speed and other key parameters to other AIS units via a VHF transceiver. The AIS, in combination with the Electronic Chart Display and Information System (ECDIS), allows the captain to view the vessel's location on a map, as well as the positions of other nearby vessels. The use of inland AISs is mandatory in many European countries [3]. The AIS is also standardized for maritime transport [4]. The information from AIS units is also received by the National River Information Services (RISs), which are used by the national inland waterway authority as a surveillance tool to manage inland waterway transport.

Though GNSS reaches very high levels of availability and continuity, due to the low power of the signal when received on Earth, GNSS is vulnerable to unintentional and intentional terrestrial sources of radio frequency interference (RFI). Intentional interference may be in the form of jamming, spoofing or beaconing signals. This AIS's vulnerability to GNSS RFI is a known issue. There have been numerous documented cases of GNSS RFI

impacting AISs. These cases include jamming in the Black Sea and around Crimea, in the sea near Syria and around Cyprus, and even cases of spoofing [5–7].

Even though these cases of GNSS RFI impacting AISs are known, the full extent of the vulnerability is not fully understood. Although a few studies have already been conducted [8–11], they were more focused on the feasibility of RFI attacks and included only one type of interference and environment. Furthermore, the impact of an either jammed or spoofed AIS unit on subsequent systems is completely unknown.

This paper presents a comprehensive vulnerability testing of the inland waterway AIS unit including jamming and spoofing tests in laboratory and live-sky environments. The paper provides performance and resilience parameters of AIS under RFI. The impact of multiple jammers differing in their jamming signal characteristics is compared. Additionally, the effect of the jammed and spoofed AIS unit on the RIS server and other vessels is described.

2. Materials and Methods

The materials and methodology used for the comprehensive vulnerability testing are divided based on the test conditions and type of interference into 3 parts: laboratory testing, jamming under live-sky and spoofing under live-sky

2.1. Laboratory Testing

The aim of the laboratory testing was to precisely measure the jamming signal power which impacts the AIS unit performance in a controlled environment. However, the impact may differ based on the jamming signal used. Therefore, two different jammers were used and compared. The AIS unit under test was a standalone unit receiving only GPS L1. The specific model number and manufacturer are intentionally not included.

GNSS simulator model GSS6700 from Spirent was used to generate an authentic GNSS signal. As a source of interference, two different types of GNSS jammers were used. The first was a commercial GNSS jammer, and the second was a jamming signal created by a DVB-T modulator DTU-315 from DekTec (Hilversum, The Netherlands) and vector generator SMA100A from Rohde&Schwarz (Muenchen, Germany). The different characteristics of the two jamming signals can be seen in Figure 1, which shows waterfall diagrams of a 160-microsecond-long sample of the signal at the 60 MHz bandwidth, centred at the 1575.42 MHz frequency.

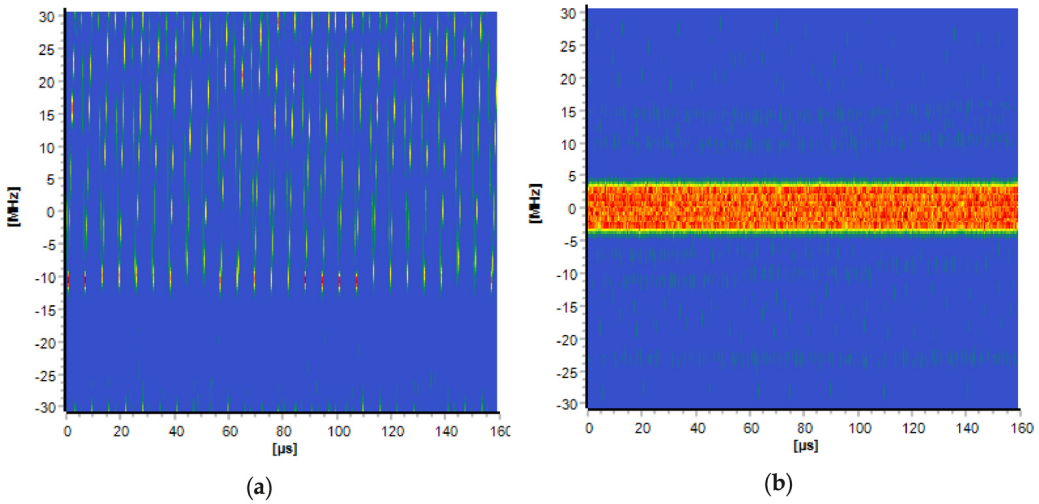


Figure 1. The waterfall diagram of the commercial jammer (**a**) and the waterfall diagram of the jamming signal created by the DVB-T modulator (**b**).

The jamming signal power was controlled by a Hewlett Packard (Palo Alto, California, United States) attenuator, model 8494B. The authentic and the jamming signal were coupled

using a signal coupler from Hewlett Packard, model 778D-012. During both scenarios, the AIS unit was connected via RF cable to the coupled signal and the unit was subjected to a slowly increasing jamming signal power. The power was increased by 1 dBm increments. The coupled signal was simultaneously monitored and analysed via a Rohde&Schwarz FSH13 spectrum analyser.

2.2. Jamming Testing under Live-Sky

The second part of the vulnerability testing took place on a 16 km long section of the river Elbe during normal operation. The AIS unit under test was on board a passenger ship called PORTA BOHEMICA (ENI: 32201626) providing a regular transport service on the river. The AIS unit under test receives only the GPS L1 frequency signal and the Differential GNSS corrections. The aim was to observe the impact of jamming on AIS, as well as how other AIS units and the RIS server will react in the presence of a jammed AIS unit.

The testing consisted of two static scenarios when a moored vessel was jammed from the shore and its deck and two dynamic scenarios when a sailing vessel was jammed from the shore and its deck. GNSS jammer model TG5CA was used for the live-sky tests. The jammer transmits at the GPS L1 frequency with 20 MHz bandwidth, has a 4.0 watts power output and its jamming signal can be characterized as a Sawtooth signal.

2.3. Spoofing Testing under Live-Sky

The third part of the vulnerability testing was very similar to the second one. The same AIS unit was tested, and the experiments were carried out at the same location. The aim was identical as well, only instead of jamming, a spoofing signal was used. The testing consisted of static and dynamic spoofing both from shore and the deck. In total, six scenarios were carried out. In two of the six scenarios, spoofing was preceded by jamming of the AIS unit. The difference between the true position of the vessel and the generated spoof position was between 100 and 1500 m, and the time difference was between a few minutes to several hours.

As a source of the spoofing signal, the portable GNSS simulator from Spirent was used. The portable GNSS simulator supports the simulation of multi-constellation and multi-frequency scenarios with up to 36 channels and a maximum RF output power level of −45 dBm. The spoofing signal generated was based on the GPS constellation transmitting at the GPS L1 frequency by using a passive transmit antenna with a 4.0 dBi gain. The RF output power level in the simulation scenarios was chosen in such a way that the target power level received by the AIS unit was −120 dBm.

2.4. Captured Data and Impact Evaluation

During all the testing, NMEA messages of the AIS unit under test were recorded together with the alerts issued by the unit. Additionally, for the live-sky testing, NMEA messages from nearby vessels and the recording of the RIS server screen were captured. To evaluate the vulnerability of the AIS unit, the following metrics were used:

- Horizontal position error (HPE);
- The number of satellites in use;
- Whether an integrity alert was issued or not;
- Time to alert;
- The ability to re-acquisition the authentic GPS signal after interference is gone;
- Time to re-acquisition the authentic GPS signal after interference is gone;
- General system behaviour and the ability to fulfil its function.

The power of the interference signal impacting the AIS unit was directly measured on a spectrum analyser in the laboratory testing and computed using the Free-space path loss formula in all of the live-sky tests. During performance testing, the HPE value did not exceed 2 m. Therefore, HPE over 2 m was considered a performance impacted by RFI.

3. Results

Similarly, to Section 2, the results of the vulnerability testing are structured into three parts based on the type of interference and test environment.

3.1. Laboratory Testing

The results of the laboratory testing are split into two sub-sections according to the jammer used.

3.1.1. Impact of the Commercial Jammer

Figures 2 and 3 show the effect of a slowly increasing jamming signal power generated by a commercial jammer on the HPE and the number of satellites in use parameters.

In Figure 2, we can observe that up to a jamming signal power of −64 dBm, the number of satellites in use corresponds to the unjammed state of the unit. From the power level of −61 dBm onwards, an increased fluctuation in the number of satellites in use and their gradual decrease is observed. From −56 dBm, the AIS unit is no longer able to receive the authentic signal in this experiment. The AIS unit displayed an alert, warning about the unavailability of the position information at a power of −57 dBm.

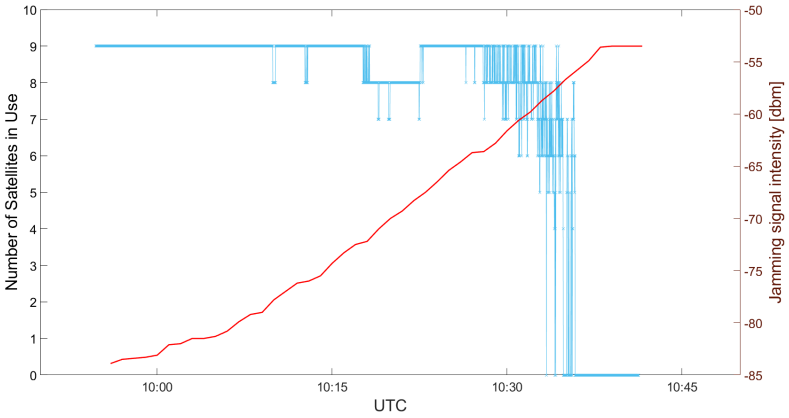


Figure 2. The number of satellites in use to calculate the position from GPS (in blue) while increasing the power of the jamming signal generated by the commercial jammer (in red).

In Figure 3, the impact of GNSS jamming on AIS performance expressed through the HPE parameter can be observed already at the power level of −70 dBm, when the HPE rises above 2 m for the first time. Up to this point, the HPE value has been kept below 1 m. From a power level of −62 dBm, the HPE value goes above 5 m. The HPE did not exceed 10 m for the duration of the experiment.

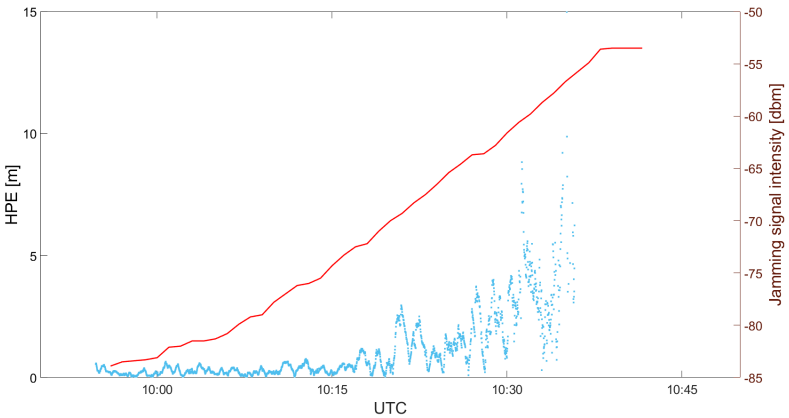


Figure 3. The horizontal position error parameter (in blue) while increasing the power of the jamming signal generated by the commercial jammer (in red).

3.1.2. Impact of the Jamming Signal Generated by the DVB-T Modulator

Figures 4 and 5 show the effect of a slowly increasing the jamming signal power generated by the DVB-T modulator on the HPE parameter and the number of satellites in use.

In Figure 4, at a jamming signal power of −71 dBm, the first decrease in the number of satellites in use by two can be observed. In the interval from −71 dBm to −68.5 dBm, the number of tracked satellites fluctuates between 6 and 11. From −68.3 dBm, the AIS unit is no longer able to track the authentic signal. At the same power, the AIS unit issued an alert, indicating a loss of position.

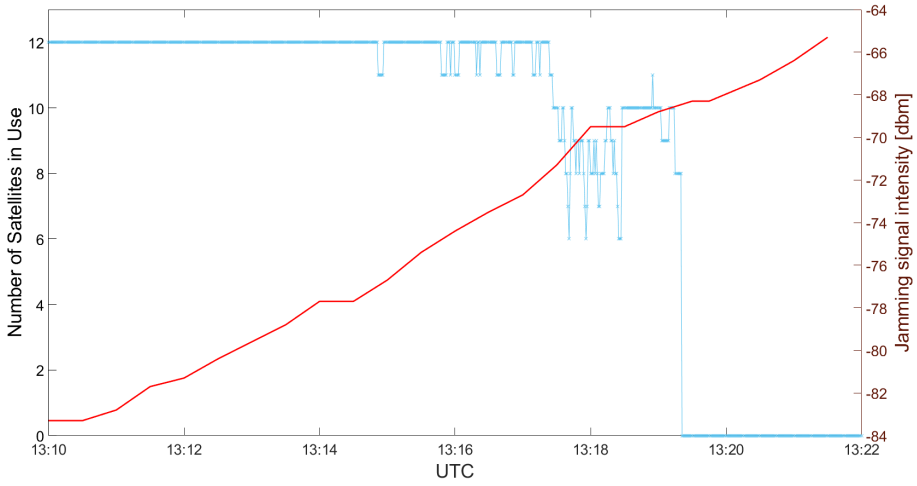


Figure 4. The number of satellites in use to calculate the position from GPS (in blue) while increasing the power of the jamming signal generated by the DVB-T modulator (in red).

In Figure 5, the interference generated by the DVB-T modulator caused an HPE greater than 2 m at −79 dBm. From −75.5 dBm, the HPE increases exponentially up to a maximum of 35 m. The HPE then decreases to the range of 10 to 20 m, which corresponds with the increase in the number of satellites in use in Figure 4. After −68.3 dBm, the HPE could no longer be computed since the unit stops reporting its position.

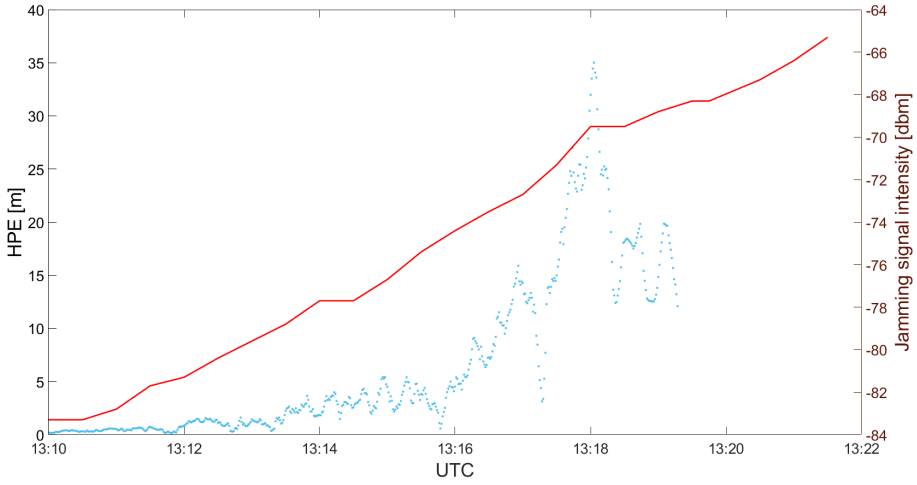


Figure 5. The horizontal position error parameter (in blue) while increasing the power of the jamming signal generated by the DVB-T modulator (in red).

3.2. Jamming Testing under Live-Sky

The AIS unit was successfully jammed during all four scenarios. The user of the unit was informed about the GPS outage in all cases. The time to alert was measured in the interval from 5 to 9 s, with a mean of 6.25 s. The unit was also able to re-acquisition the authentic GPS signal once the jamming was turned off. The time to re-acquisition was

measured between 2 and 3 s. Nevertheless, the position was displayed on the AIS screen much later, specifically 7 to 8 s after the jamming ceased. The jamming signal power at which the AIS unit loses track of the authentic signal and later regains it was evaluated during one of the dynamic scenarios. Figure 6 shows the number of satellites in use while the vessel was approaching the jammer, passing it and moving away from it.

In Figure 6, with the gradual increase in the jamming signal power, the number of satellites in use starts to fluctuate and decrease. The loss of position occurs when the number of satellites in use drops below four, which corresponds with the signal power of −49.5 dBm. Once the vessel passed the jammer, the signal power gradually decreased. The first re-acquisition occurred at −50.5 dBm. However, a stable position reading in NMEA messages was reached later, when the power was reduced to −56.2 dBm.

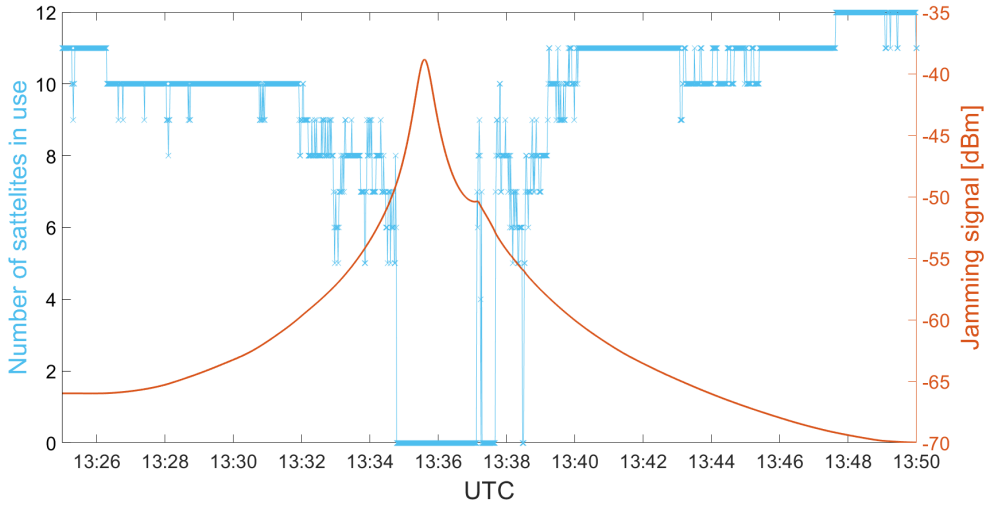


Figure 6. The number of satellites in use during a dynamic scenario when the vessel was approaching and moving away from a jammer on the shore of the river.

3.2.1. Impact on the RIS Server

Despite the absence of a position reading from the jammed AIS unit, the jammed vessel did not disappear from the RIS server screen. The jammed vessel remained visible at its last reported location. The vessel remained motionless for over 15 min until the unit was no longer jammed. Once no longer jammed, the vessel marker "jumped" to the newly reported location. No alert or warning was provided by the RIS server during the entire experiment.

The time between the first NMEA message containing the vessel position after the re-acquisition of the authentic GPS signal and the update of the vessel position on the RIS server screen were also measured. The time to update the vessel position was between 8 and 26 s with a mean of 14.5 s.

3.2.2. Impact on the Nearby Vessels

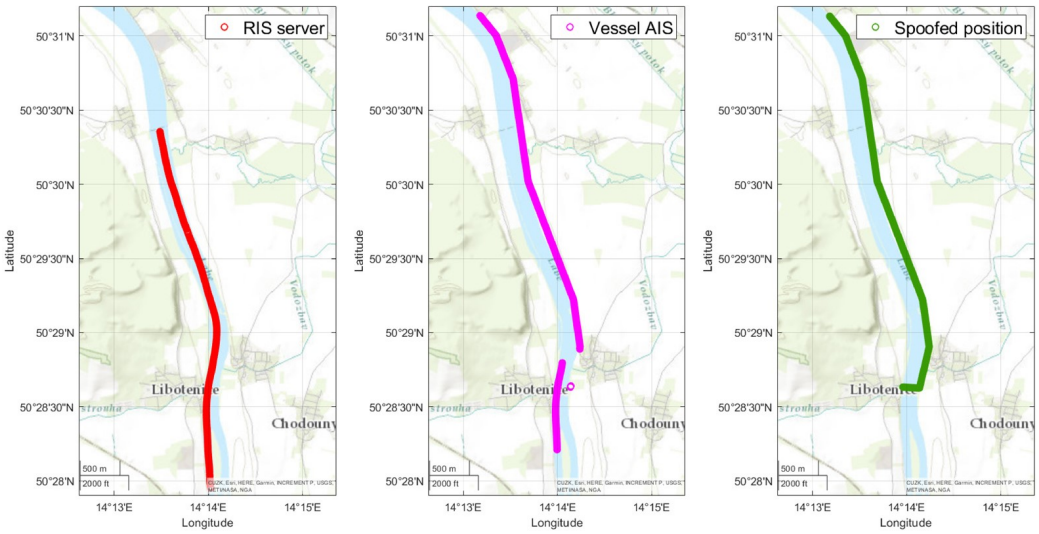
Once the AIS unit under test was jammed and unable to compute its position, its marker simply disappeared from the nearby vessels' screens. The captains of nearby vessels were not informed about the disappearance in any way.

3.3. Spoofing Testing under Live-Sky

None of the scenarios, when the spoofer was located at the shore, were successful. Conversely, all spoofing scenarios from the deck were successful.

3.3.1. Impact of Spoofing-Only Attack

In Figure 7, the impact of spoofing is evaluated by comparing the vessel trajectory from three different sources: the RIS server, the AIS unit NMEA messages and the spoofed trajectory. As Figure 7 demonstrates, shortly after the spoofer was turned on, in the city of Libotenice, the AIS unit started tracking the spoofed signal rather than the authentic one and began to report the counterfeit location. However, this spoofed location did not translate into the RIS surveillance situation.



(**a**) (**b**) (**c**)

Figure 7. Comparison of vessel trajectories from three different sources: the RIS server (**a**), the AIS unit under test (**b**) and the spoofer (**c**) during the spoofing-only attack.

Despite the AIS unit transmitting the spoofed location, the RIS server displayed the real position of the vessel. During this scenario, the AIS user was alerted to the spoofing by a time synchronization error. The difference between the authentic UTC time and the spoofed time was in the order of hours. After the spoofer was turned off, the unit under test was not able to recover and required a manual restart to start tracking the authentic GPS signal.

3.3.2. Impact of an Attack Combining Jamming and Spoofing

In this scenario, the time difference between the authentic UTC time and the spoofed time was reduced to a few minutes, and the spoofing was preceded by strong jamming. The impact of this combined attack on the RIS server and the AIS under test is showcased in Figure 8. The combined attack led to the AIS unit tracing the spoofed signal. The RIS server displayed partly the authentic location which drifted into the land once the vessel approached the location generated by a spoofer. After the spoofer was turned off, the unit under test was not able to recover and required a manual restart.

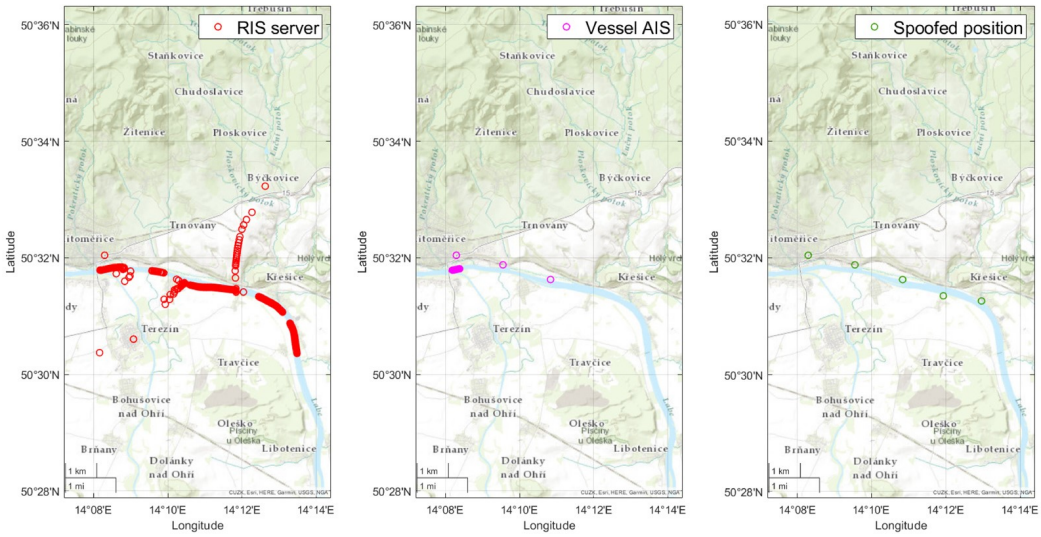


Figure 8. Comparison of vessel trajectories from three different sources: the RIS server (**a**), the AIS unit under test (**b**) and the spoofer (**c**) during the attack combining jamming and spoofing.

4. Discussion

The results presented in Section 3 clearly demonstrate the AIS's vulnerability to GPS jamming and spoofing and describe it in great detail. The impact on performance was first detected in the range of the jamming signal power from −79 dBm to −70 dBm depending on the type of jamming. The jamming signal power when the AIS unit loses complete track of the GPS satellites was measured within the interval from −68.3 dBm to −49.5 dBm based on the jammer used. Overall, it was observed that the degree of vulnerability and the impact on performance is greatly dependent on the character of the jamming signal.

An HPE of up to 35 m was measured during the experiments. Unfortunately, the user was not alerted about any decrease in performance. On the other hand, the user was informed about the complete loss of the GPS signal within 9 s at the latest after the loss of the signal occurred.

The spoofing attacks in multiple cases manipulated the vessel output which shows that spoofing is a real threat to AISs. The AIS unit also required a manual restart to recover from the spoofing attacks. Unless the spoofing was preceded by jamming and the time difference was in the order of minutes the unit did display a time synchronization warning message.

The RIS operator was not informed about the absence of position information from the jammed vessel in any way. The jammed vessel stayed "frozen" in the last reported location. Such misinformation may cause issues in inland waterway transport management. On the other hand, the vessel under spoofing-only attack had no effect on the RIS server which kept displaying the true position of the spoofed vessel. This result was surprising since, according to the research team's knowledge confirmed by the operator of the system, the AIS units are the only source of position for the RIS server. However, once the spoofing was preceded by jamming, even the RIS server was affected, resulting in the vessel position drifting in seemingly random directions. At one moment, the vessel position was displayed over 100 km away from its true location.

In regards to the impact of jammed and spoofed vessel on other AIS units, when subjected to jamming, the vessel simply disappeared from the screens of other AIS units. Captains of unjammed vessels were not alerted in any way about this disappearance. This may create a hazardous situation in conditions of reduced visibility, like foggy weather. When the vessel under test was subjected to successful spoofing, nearby AIS units displayed the spoofed location of the spoofed vessel.

5. Conclusions

This paper presents the results of a comprehensive GNSS RFI vulnerability testing of the AIS system. The results also describe the effect of the jammed or spoofed AIS unit on subsequent systems. The results provide valuable insight into the vulnerability of inland waterway transport. The paper provides a basic scheme which can be followed and/or adapted for future testing of the vulnerability of other CI systems.

The results presented are limited by the available hardware. In light of the presented results, vulnerability tests shall be conducted using a pre-determined set of jammers, each representing a common jamming signal characteristic. Additionally, having a spectrum analyser present at the spoofing testing might answer why some of the spoofing scenarios failed and bring more insights into the system's resilience.

The presented vulnerability testing was limited to a stand-alone AIS unit and to a vessel with an AIS unit as the only positioning system. However, more sophisticated vessel systems can combine AIS unit information with other technologies such as radar. Unfortunately, at the time of testing, no vessel with such equipment was available. Therefore, vulnerability testing of these vessels is recommended for future research.

Having in mind the trend of maritime and inland waterway transport of implementing more autonomous systems, where GNSS is a key source of PNT, vulnerability testing similar to the one presented in this paper shall be conducted to understand the vulnerability to GNSS RFI and its effects.

Author Contributions: Conceptualization, T.D.; methodology, J.S., J.H. and T.D.; software, J.S.; formal analysis, J.S. and J.H.; investigation, J.S., J.H., T.D. and G.H.; resources, T.D. and G.H.; data curation, J.S.; writing—original draft preparation, J.S. and J.H.; writing—review and editing, J.H., T.D. and G.H.; visualization, J.S.; supervision, T.D.; project administration, T.D.; funding acquisition, T.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the European Space Agency (ESA), specifically the NAVISP program element 3, project name "GNSS Vulnerability and Mitigation in Czech Republic".

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The laboratory testing was performed in collaboration with the Research Institute of Posts and Telecommunications in Slovakia. The Inland Waterway Authority of the Czech Republic provided the team with the standalone AIS test unit and participated in the live-sky testing.

Conflicts of Interest: Author Günter Heinrichs was employed by the company Spirent Communications, Crawley, UK. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AIS	Automatic Identification System
CI	Critical Infrastructure
ECDIS	Electronic Chart Display and Information System
ESA	European Space Agency
GNSS	Global Navigation Satellite Systems
HPE	Horizontal Position Error
PNT	Positioning, Navigation and Timing
RFI	Radio Frequency Interference
RIS	River Information Services

References

1. *EUSPA EO and GNSS*; Publications Office of the European Union: Luxembourg, 2022; Volume 2022. [CrossRef]
2. Whitty, C.; Walport, M. *Satellite-Derived Time and Position: A Study of Critical Dependencies*; Government Office for Science: London, UK, 2018.
3. *Commission Implementing Regulation (EU) 2019/838 of 20 February 2019 on Technical Specifications for Vessel Tracking and Tracing Systems and Repealing REGULATION (EC) No 415/2007*; European Commission: Brussels, Belgium, 2019.
4. *SOLAS—International Convention for the Safety of Life at Sea: Chapter V-Safety of Navigation, Regulation 19*; International Maritime Organization: London, UK, 2002.
5. *Above Us Only Stars: Exposing GPS Spoofing and Jamming in Russia and Syria*; C4ADS: Washington, DC, USA, 2019.
6. *Resolution MSC.428(98)*; Maritime Cyber Risk Management in Safety Management Systems. International Maritime Organization: London, UK, 2017.
7. *GPS World: Moves ship Locations Thousands of Miles*; GPS World: Cleveland, HI, USA, 2020.
8. Androjna, A.; Perkovič, M.; Pavic, I.; Mišković, J. AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Appl. Sci.* **2021**, *11*, 5015. [CrossRef]
9. Caprolu, M.; Pietro, R.D.; Raponi, S.; Sciancalepore, S.; Tedeschi, P. Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. *IEEE Commun. Mag.* **2020**, *58*, 90–96. [CrossRef]
10. Grant, A.; Williams, P.; Ward, N.; Basker, S. GPS Jamming and the Impact on Maritime Navigation. *J. Navig.* **2009**, *62*, 173–187. [CrossRef]
11. Medina, D.; Lass, C.; Marcos, E.P.; Ziebold, R.; Closas, P.; Garcia, J. On GNSS Jamming Threat from the Maritime Navigation Perspective. In Proceedings of the 2019 22th International Conference on Information Fusion (FUSION), Ottawa, ON, Canada, 2–5 July 2019. [CrossRef]