Guiding Ship Navigators through the Heavy Seas of Cyberattacks

Merlin von Rechenberg[•], Nina Rößler[○], Mari Schmidt[•], Konrad Wolsing[•*], Florian Motz[○], Michael Bergmann[†], Elmar Padilla[•], and Jan Bauer[•]

[•]*Cyber Analysis & Defense*, *Fraunhofer FKIE*, Wachtberg, Germany · {firstname.lastname}@fkie.fraunhofer.de

[○]*Human Systems Engineering*, *Fraunhofer FKIE*, Wachtberg, Germany · {firstname.lastname}@fkie.fraunhofer.de

[*]*Communication and Distributed Systems*, *RWTH Aachen University*, Germany · {lastname}@comsys.rwth-aachen.de

[†]*BM Bergmann Marine*, Grosskrotzenburg, Germany · michael.bergmann@bergmann-marine.com

***Abstract*—The entire maritime sector, encompassing not only on-shore systems but especially systems onboard vessels, is increasingly endangered by threats from cyberspace. Implementing preventive security like cryptography into existing systems can be costly. Thus, network-based Intrusion Detection Systems (NIDSs) promise to be a retrofittable security solution that alerts suspicious network behavior. Regarding vessels, however, there is still a lack of NIDSs detecting sophisticated cyberattacks manipulating nautical data, e.g., by spoofing a vessel's course and position. Moreover, the intended users of such NIDSs onboard vessels would be nautical operators rather than cybersecurity experts, although interpreting the alarms of a typical NIDS and understanding their consequences requires expert knowledge in cybersecurity. For this reason, we present a *Cyber Incident Monitor (CIM)*, a security framework combining a specialized maritime NIDS to detect sophisticated attacks in maritime networks with a customized human machine interface (HMI) providing tailored guidance for nautical operators to respond adequately in the event of a cyberattack. Using simulations, we show that CIM detects attacks quickly and through usability tests involving nautical experts, we derive helpful advice for the HMI development. Overall, CIM enables the detection of maritime cyberattacks while providing alerts and recommendations to navigators to take appropriate measures in a timely manner.**

***Index Terms*—Maritime Cybersecurity; Intrusion Detection System; Integrated Bridge System; IEC 61162-450; NMEA 0183**

I. Introduction

Commercial shipping is essential in world trade and global supply chains and is expected to grow drastically by 2050 [11]. With ongoing digitalization in the commercial shipping industry, the surface for cyberattacks increases [5]. Consequentially, cyberattacks are considered to be a major threat to the industry by the maritime community [24]. Reported incidents further confirm this concerning and emerging trend [17].

Whereas attacks against on-shore logistics infrastructures have been known to cause great economic damage in the past [23], recently, various cyberthreats on maritime systems onboard vessels have been successfully demonstrated, including attacks against integrated bridge systems (IBSs) [14], the automatic identification system (AIS) [2], global navigation satellite systems (GNSSs) [3], marine radar [29], and satellite-based communication [20]. Attacks onboard vessels are particularly dangerous as they can impact global supply chains, similarly to the Suez Canal obstruction in 2021 [13], but more seriously threaten environmental safety, crews, and passengers, e.g., by manipulating a vessel's position to lure it into shallow waters. Hence, maritime organizations have recognized the urgent demand for cybersecurity [10], and research on maritime cybersecurity is increasingly concerned with developing appropriate methods to prevent cyberattacks or at least to avoid incidents from remaining undetected [26]. Yet, complete prevention of cyber incidents is generally utopistic to achieve in practice. As one step toward prevention, the IEC 61162-460 standard proposed methods for higher safety and security than achieved by IEC 61162-450 [8] and NMEA 0183. Still, retrofitting such mechanisms into existing systems is costly. For defense-in-depth, cyber risk assessments show that additional measures must be implemented [4].

One detection mechanism that fulfills these needs and is retrofittable to existing systems without requiring the cumbersome exchange of hardware, are network-based Intrusion Detection Systems (NIDSs). These monitor the network traffic and alert suspicious messages. Well-established tools such as Snort [22] or Zeek [25] perform best in traditional computer networks, like datacenter, office networks, or on-shore IT infrastructures since those tools are primarily designed for signature-based misuse detection. However, detecting stealthy attacks with seemingly valid messages but slightly modified contextual information, especially on the application layer of domain-specific protocols, requires more effort [27].

Besides reliably detecting cyberattacks, current NIDSs lack specific guidance on actions to take after they indicate a potential incident. This is especially crucial in maritime scenarios onboard vessels where usually no trained personnel exists to mitigate cyberattacks. Yet, for the crew to maintain situational awareness, they need to know which electronic instruments they can still rely on to operate their vessel safely.

To detect specialized attacks against a vessel's navigational information and to simultaneously guide nautical operators on how to cope with the incident in a specific solution, we propose a novel NIDS framework for IBSs based on the IEC 61162-450 and NMEA 0183 protocols, called *Cyber Incident Monitor (CIM)*. CIM is tailored to the specific requirements of maritime systems, which eases its deployment into existing shipboard networks. Moreover, our framework provides an ergonomic human machine interface (HMI) to enable nautical operators to quickly assess the extent of detected incidents and the resulting

risks and initiate suitable response measures. To validate CIM practically, we conduct a performance evaluation of the NIDS and a user evaluation for the HMI. Overall, CIM provides a security solution that helps a vessel's crew to retain situational awareness through the emerging heavy seas of cyberattacks.

II. Background & Related Work

The art of unveiling harmful cyberattacks via intrusion detection constitutes an own field of research [28], which can be divided into two major directions. *Misuse detection* defines abnormal behavior with attack signatures and tries to re-identify them, e.g., in the network. While this paradigm provides high accuracy in searching for specific attack patterns, i.e., recurring malware in traditional office networks, misuse detection is limited to identifying known attacks only. Thus, it is less suited for maritime NIDS applications where attacks can uniquely target a single vessel and even dynamically adapt to navigational situations [29]. In contrast, *anomaly-based* detection trains a model of normal behavior, alerts deviations from the expected patterns, and is therefore able to expose unknown attacks. Still, a comprehensive model of normal behavior is required to avoid false-positives. For maritime scenarios onboard vessels, anomaly detection nonetheless promises to detect a wide variety of cyberattacks.

Within the research community, anomaly detection has already been widely studied and proven successful, especially for cyber-physical systems [6], [19]. While approaches from this field could be transferred to the maritime domain, they lack the essential understandability of alerts necessary to retain situational awareness among the crew. Regarding specialized approaches, Riveiro et al. conducted a survey on the state-of-the-art in maritime anomaly detection [21], concluding that approaches analyzing the network topology of maritime systems exist, but none of them represents a NIDS. More recently, Amro et al. proposed multiple techniques to reliably detect attackers in nautical communication [1]. Yet, their NIDS represents a technical approach that does not account for nautical users, for whom it is unlikely to be security experts.

Concerning the integration of a maritime NIDS into a ship's bridge, however, different requirements and standards exist w.r.t. HMIs. For HMIs specifically tailored to navigators, various requirements arise from the context of use on the ship's bridge. In particular, they must comply with the IMO performance standards for bridge alert management [9]. The standards specify, among others, the prioritization of issued alerts, the visual and acoustic signaling, as well as required functionalities to mute and acknowledge alerts.

To the best of our knowledge, there exists no maritime NIDS suitable for integration into ships' bridges that simultaneously takes into account the unique needs of navigators who must assess incident alerts to determine the resulting risks and make time-critical decisions about how to respond.

III. Cyberthreats & Threat Model

To protect maritime systems, novel NIDSs that integrate seamlessly into a vessel's bridge are required. Yet to design new detection methodologies, it is crucial to understand the individual cyberthreats and attack models.

Various attack vectors exist against maritime systems to obtain access to the internal network, which is responsible for distributing the navigational information from sensors to the HMIs in the bridge. First, compromising insecure public-facing (wireless) interfaces, e.g., satellite communication, VHF, GNSS, AIS, radar, can serve as the first entry point for an attacker [5]. Also, physical access to the vessel and its network components, e.g., by injecting malware via USB ports [15], but also by introducing malicious devices or conducting supply chain attacks [16], directly enables attackers to perform internal attacks.

Once attackers obtain access to the internal communication network, they can attack the distribution of nautical data. Sensors perceiving the environment broadcast updates to the bridge, which get aggregated into a situational picture. Consequently, an adversary can manipulate the situational picture perceived such that it no longer corresponds to the actual state of the vessel. Moreover, widely used legacy protocols IEC 61162-450 [8] and NMEA 0183 lack essential protection of confidentiality, integrity, and authenticity due to missing cryptography which would protect that sensitive data [14].

To ultimately launch a cyberattack against these insecure communication protocols, an attacker has two options. First, a machine-in-the-middle (MitM) position with full access to the (unencrypted) communication enables eavesdropping, message injection or even interception, and manipulation of messages sent by authorized devices. Thus, a sophisticated MitM attacker is generally hard to detect [1]. However, MitM attacks' success depends on the position within the network and also requires knowledge about the specific maritime system under attack, thus, is complex to accomplish. Second, a machine-on-the-side (MotS) attack can take place anywhere on the network but with reduced capabilities. Interception and manipulation of messages sent by others is not directly possible. However, due to the unique broadcasting property of maritime network protocols, this does not reduce the attackers' capabilities. They can still distort navigational information arbitrarily [7]. Therefore, MotS attacks are more realistic and more likely to occur, which is why we focus on this attack type hereinafter.

Overall, a MotS attacker can gain complete control over the situation picture in a maritime network. This includes, but is not limited to, manipulations of position, course, heading, speed, depth, and AIS data, which can cause serious navigation failures leading to economic or environmental damage, endangering human lives, demanding proper security mechanisms.

IV. Cyber Incident Monitor

To improve security against cyberattacks while aiding navigational operators, we introduce CIM, our *Cyber Incident Monitor*, which monitors nautical communication. CIM is based on a maritime NIDS tailored for IBSs and an ergonomically designed HMI (cf. Figure 1). The NIDS, deployed in the bridge network, performs the anomaly detection (cf. Section IV-A). Indications of cyberattacks from the NIDS are

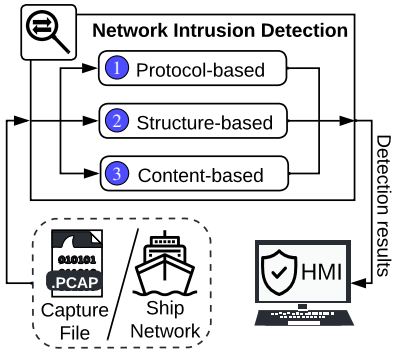


Fig. 1. Cyber Incident Monitor combines multivariate NIDS with an ergonomic HMI to visualize the detection results and provide contextual advice.

forwarded in real-time to the ergonomic HMI installed at the bridge, providing alerts to navigators (cf. Section IV-B). Combining both mechanisms into CIM promises to improve the current situation of endangered vessels as shown in our evaluation (Section IV-C).

A. Maritime NIDS

Since MotS attacks pose a serious threat to the safe operation of current maritime systems (cf. Section III), we develop a maritime NIDS to detect such attacks. As shown in Figure 1, the NIDS implements three fundamental detection methods: (1) protocol-based approaches identify denial of service attacks and unusual frequencies of regularly occurring messages, (2) structure-based alerts indicate violations to a predefined or the observed network topology, and (3) content-based approaches test the plausibility of transmitted values against a physical model, indicating abnormal deviations.

The *protocol-based* detection method is based on the finding that MotS attacks typically require a higher frequency to successfully manipulate the situation picture [7]. This is because the MotS position does not allow suppressing legitimate messages. Consequently, by flooding the network with manipulated messages, legitimate messages are being discarded by the IBS, either because they are presumed to contain measuring errors in integrity checks or because the sampling rate of the processing systems is too low [7]. Since the frequencies of legit messages are usually well-defined and static in a maritime environment, attacks can be detected by monitoring the current message frequencies and searching for frequency anomalies, i.e., abnormal frequencies of an individual message type.

Next, the *structure-based* detection uses a model of the network topology defined as a ruleset to monitor the actual topology and search for anomalies. Each rule defines an expected or allowed combination of different types of meta information that should be found in a message. The meta information can include common IP/UDP source and destination identifiers such as MAC and IP addresses or ports but it can also incorporate information related to the special maritime protocols, like source tags from the IEC 61162-450 protocol or Talker-IDs from the NMEA 0183 standard.

Lastly, the *content-based* detection uses a physical model of the vessel to check the sensor data for plausibility, e.g., a position change is bound by the maximum speed. Based on that physical model, it is feasible to define an expected maximum plausible difference. The NIDS then searches for anomalies by comparing the actual difference between pairwise sensor measurements received in consecutive messages of the same type within a given time window. Since we assume a MotS attack, there will eventually be two consecutive messages of the same type of which one message is benign (originates from an authorized device) and one is malicious (injected by the attacker). If the attacker manipulates the situation picture, comparing those two messages fails the plausibility check and the attack is detected. However, especially in the content-based detection, false-positives can occur due to natural noise and sensor measurement errors. Thus, the mechanism only considers detected anomalies as actual attack indications if a predefined threshold of multiple anomalies is exceeded in a certain time window. Nevertheless, the threshold should be as small as possible to avoid discarding true-positives.

Any alert of the three detection methods indicates a malicious activity that is forwarded to the HMI (cf. Figure 1). Since these alerts can be ascribed to a specific anomalous behavior, it is possible in the following to provide contextual alerts and advice to the navigational operators of the vessel.

B. Ergonomic HMI

CIM's ergonomic HMI, designed explicitly for nautical operators, presents alerts about detections by the NIDS in a manner familiar to the user. Figure 2 shows a schematic overview of the HMI's design, and Figure 4 depicts the actual HMI. The basis for the display are specific alert messages defined by us for the various NMEA message types that may be affected. We have classified these alerts in terms of priority according to the IMO performance standards for bridge alert management [9] into *alarms*, *warnings*, and *cautions*.

The user interface comprises two main sections, one to display the active cyberalerts and one for the cyberalert history. The proportion of both sections can be adjusted by the users, depending on whether they decide to concentrate on the current situation or past incidents. The top of the active alerts section provides an overview of the number of currently active alerts, divided into three priority levels. In the visualization, these priority levels are redundantly coded through color and shape to enable fast and easy differentiation. A scrollable list of active alerts is located below the overview. They indicate which navigational data may no longer be trustworthy as a result of a possible cyberincident. This list shows each alert's priority, a concise alert title, the time the alert occurred, an identification number, detailed information regarding the alert cause, and the supposed network source device of the alert. The list is sorted by priority, i.e., the most critical alerts are presented at the very top. New warnings and alarms are displayed flashing and are accompanied by an audible signal to draw the attention of the bridge crew to the critical situation. As specified in the IMO performance standards [9], they can

Fig. 2. Schematic layout of CIM's HMI with two main sections for active cyberalerts including decision support (top), and cyberalert history (bottom).

be acknowledged using the checkbox in the "ACK" column, which stops the flashing and the audible signal. Moreover, all alerts can be muted for 30 seconds using the mute button.

Alerts can be selected by clicking on the respective row in the alert list. The selected alert is highlighted in blue, and the corresponding recommended countermeasures are displayed as a checklist below. These instructions serve as decision support and aim at making the effects of an attack manageable. They are generally structured as follows: First of all, they state which information may no longer be trustworthy, e.g., after the NIDS identified a potential attack on the position: "Do not trust GPS position information shown on any device (ECDIS, conning display, etc.) except original sensor display". Secondly, they support navigators in verifying the potentially corrupted information and propose alternate data sources to safely continue the journey, e.g., "Verify position if possible by taking visual bearings". Lastly, they include steps to restore the bridge systems to a normal state, e.g., "Exclude source device from network".

As soon as the cause of an alert no longer exists, the system moves the alert to the history. If there are currently no active alerts, the system informs the users that no cyberincidents have been detected and no actions are required. The history list supports the investigation of past incidents and shows the same information as the active alerts list, plus the time when the alert has been acknowledged. By default, the alert history is sorted by the time the alerts occurred. Similar to the active ones, alerts in the history can be selected, whereby they are highlighted and the actions taken are displayed. To ensure that the currently relevant information is quickly available to the nautical operators even with a large number of past alerts, filtering and sorting options are implemented in the history header. Using the search field, it is possible to search for key words in the alert titles, details, and sources. Only the alerts that contain the searched characters remain displayed in real-time. The data presented in the alert history can be exported for further analysis using the export button. Lastly, the order and width of the columns in the history list are customizable.

To effectively increase the safety on board, CIM should offer a high level of usability. Thus, not only the NIDS detection methods but also the HMI were subject to evaluation.

TABLE I
NIDS EVALUATION OVERVIEW: ATTACKS AND DETECTION TIMES

Attack		**Max. time until detection** (seconds)					
		① **protocol-based**		② **structure-based**†		③ **content-based**	
Manipulated parameters	**NMEA messages**	**J***	**C**•	**J***	**C**•	**J***	**C**•
Position (+0.5' N/E)	GGA, GLL	1	1	1	1	1	10
Depth (+10m)	DBT, DPT	1	1	1	1	1	10
Heading, course (+90°)	HDT, HDM, VTG	1	1	1	1	1	10
Heading, course (+90°) w/ consist. ROT	HDT, HDM, VTG, ROT	–	1	–	1	–	10
Speed (×1.5)	VTG, VBW	1	1	1	1	1	20
AIS position (+0.5' N/E)	VDM	1	–	1	–	1	–
AIS place ship in course	VDM	1	–	1	–	1	–

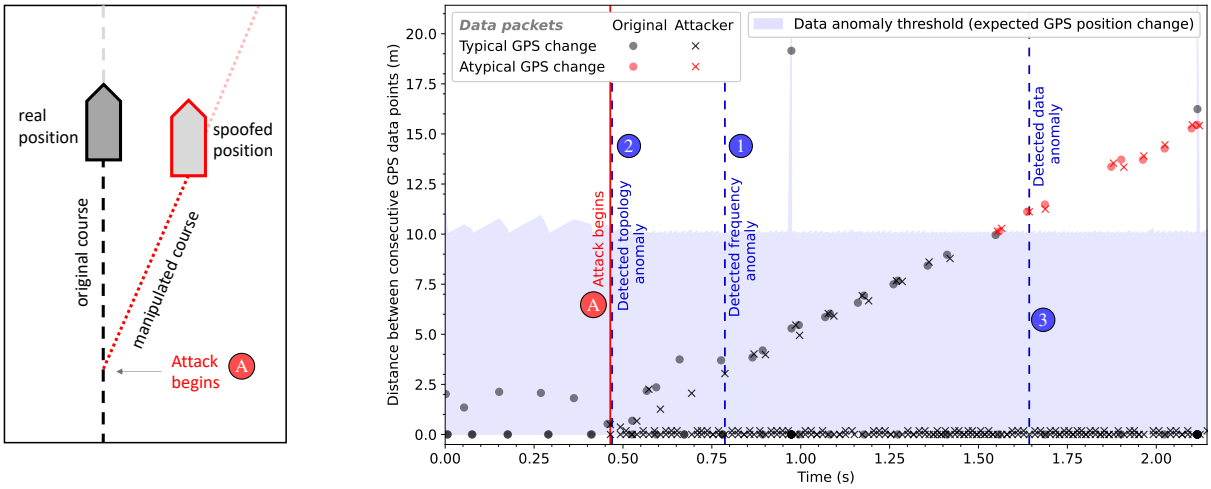
† Structure-based detection fails if the attacker spoofs authentic sender information.
* Jumping shift: attacker changes the parameter to the target value immediately.
• Continuous shift: attacker changes the parameter gradually over a 10 min duration until the target value is reached to be more stealthy.
– Attack not possible under the specific conditions.

C. Evaluation

To evaluate CIM, a testbed resembling a realistic maritime network is required. As the basis, we utilize *Bridge Command* (www.bridgecommand.co.uk), an open-source tool used to train navigational skills, that simulates realistic scenarios and generates corresponding network traffic. Furthermore, the chart plotter *OpenCPN* (www.opencpn.org) represents the IBS displaying navigational data and helps to verify the success of the conducted attacks. Cyberattacks against the network communication were performed with the *BRidge Attack Tool (BRAT)* [7], which is dedicated to simulating realistic attacks and has already been used for security research. Finally, CIM, i.e., the NIDS and the HMI, have been integrated into this environment via a virtualized network. The following evaluation of CIM is split into proving the effectiveness of the NIDS and the usability of the HMI.

1) Detection Performance of the NIDS: To investigate the effectiveness and detection speed of the NIDS, we utilized BRAT and conducted eight MotS cyberattacks within our testbed, affecting various message types of the NMEA 0183 protocol. BRAT attacked different sensors, including the position, depth, heading, course, rate-of-turn, and speed, as well as AIS data received from other vessels to manipulate their supposed positions displayed on the chart plotter. The attacks manipulating the sensor data of the own vessel were carried out in two different ways. Firstly by letting the parameters jump directly to the attackers target value and secondly by adjusting them continuously until the target value is reached.

As shown in Table I, the NIDS can detect each attack reliably and across all three detection methods. More importantly, the detection time is adequate, with the majority of the attacks being uncovered within less than one second. Especially the protocol- and structure-based detections are constantly quick. Only the detection time for a few content-based scenarios is significantly slower, implying that the difference between manipulated and original data is not significant enough to



(a) Attack. (b) Detection.

Fig. 3. CIM is capable to detect an exemplary GPS manipulation attack (a) conducted by a network-level adversary that injects malicious data into the network. Our technical evaluation (b) demonstrates the different detection methods of CIM's NIDS-based anomaly detection whose indications are passed to the navigator-centric HMI (cf. Figure 4).

be detectable at first. More precisely, the difference is still within the expected variance for the sensor measurements and thus probably even too small for a human to notice at this point. Therefore, it can be assumed that the impact of the manipulation on navigation is also still limited during the time before the detection. In conclusion, the NIDS's detection performance and speed are sufficient to give navigational operators a timely and precise alert.

2) HMI: To highlight the interaction of CIM's NIDS and its HMI component, we briefly show a simulated GPS manipulation attack (cf. Figure 3(a)) where the adversary attempts to slowly but continuously change the displayed position of the vessel by superimposing forged position data starting at A. Even a stealthy, i.e., slow-growing deviation from the original course induced by the attacker as depicted here, is detected promptly by CIM (cf. 1 to 3 in Figure 3(b)). Shortly after the detection, the corresponding alerts are issued to the navigator, as shown in Figure 4, accompanied by recommended actions to perform in that situation.

Since we followed a human-centered design approach [12] in developing the HMI, several iterations were performed starting from defining user requirements, through designing initial prototypes, to implementing the final application. This included a formative evaluation in which four nautical experts participated, aimed at determining how well the system is tailored to user requirements and how intuitively understandable and usable it is from a navigator's standpoint. Due to COVID-19 restrictions, the evaluation was only possible as a remote usability test with a limited number of four subjects. Still, we fulfill the number of minimum required subjects for such a study as recommended by Nielsen [18]. By observing, employing the think-aloud protocol, and conducting post-session interviews, we could elicit suggestions for improving the usability, which were incorporated in the final version of CIM. Similarly, the presented decision support has been

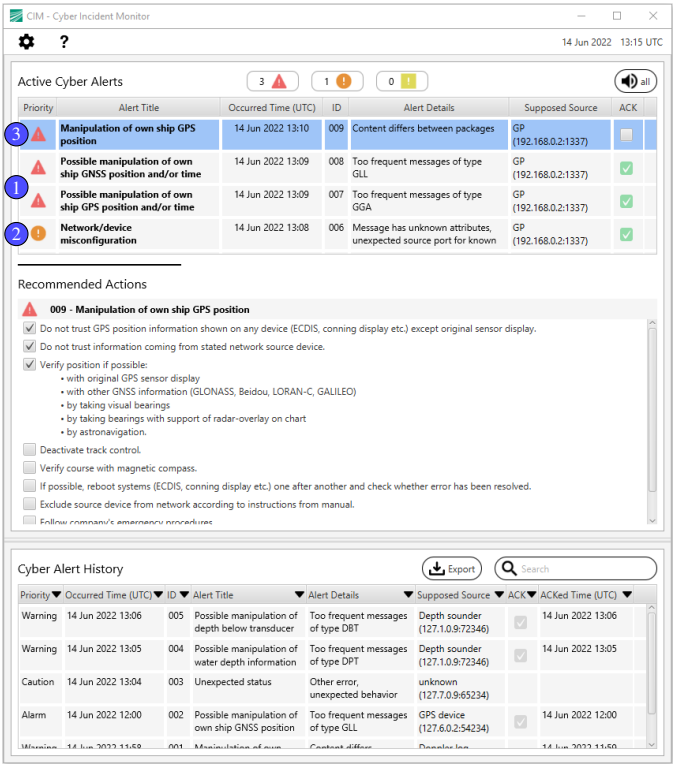


Fig. 4. Navigator-centric HMI that alerts and instructs bridge crews in case of cyberincidents based on the indications of the NIDS.

defined and refined in several interviews with nautical experts to ensure that the recommended measures are both adequate and practicable for navigators.

Overall, with CIM, we have developed a NIDS framework tailored to IBSs that detects anomalies in the communication of nautical data and guides navigators through an ergonomic and human-centered HMI.

V. Discussion

As explained in Section III, our approach focuses on detecting internal MotS attacks. Hence, an external attack that affects the sensors and manipulates the measurements before they are sent via the internal network may not be detectable by CIM. Internal MitM attacks are likewise difficult to detect if the attacker carefully designs the attack [1], i.e., a MitM attacker can intercept and modify messages without flooding the network with malicious ones as a MotS attacker. While this would circumvent the protocol- and structure-based detection of CIM, the content-based approach can theoretically identify the attack as long as the modifications are large enough, i.e., introducing notable jumps in the data. Improving the latter type of detection should be part of future work, e.g., by making the physical model more complex, tailoring it to a specific vessel, enabling holistic cross-parameter plausibility checks, or even adapting complex detection methodologies from related branches of cyber-physical system security research. Lastly, fusing the indications of the three detection mechanisms might further reduce false-positives and increase reliability. Openly available data sets are also desirable for further research and generalizable as well as comparable results.

Regarding the HMI, an in-depth (summative) evaluation could be conducted with a larger sample size, allowing detailed statistical analyses based on responses to a standardized usability questionnaire. Concerning practical use on board, it would be interesting to investigate the interoperation of CIM with existing bridge systems. In future studies, both the detection mechanisms and the HMI should be investigated not only in simulated environments but also in real-world scenarios onboard vessels. Since the attention of navigators typically shifts between various navigational and safety systems and they now have additionally to deal with the impact of cyberattacks, their workload should also be considered in future work in addition to technical issues. Similarly, dynamic, situation- and mission-specific prioritization of recommended actions in the HMI would be useful to further support crew response capabilities in the event of an attack.

VI. Conclusion

Sophisticated maritime cyberattacks against nautical data pose a serious threat to the operation of vessels endangering global trade, crews, passengers, and the environment's safety. To this end, we propose our retrofittable Cyber Incident Monitor (CIM), which not only detects stealthy cyberattacks reliably but simultaneously provides swift aid and recommended reactions to the crew in a single solution. In a synthetic evaluation, CIM only requires about one second to detect and notify an incident to the crew. Moreover, the interface to nautical officers has been validated for ergonomics and the provided incident response instructions were refined for expedience in a user study together with maritime experts. Overall, CIM enables even crews not trained in cybersecurity to respond appropriately and timely to cyberincidents and ultimately maintain situational awareness of their vessel's state, which significantly increases overall operational safety.

Acknowledgments

The work in this paper was partially funded by the German Federal Ministry for Digital and Transport (BMDV) as part of the project SINAV (project 40.0404/2019). Additionally, the authors thank the German Federal Maritime and Hydrographic Agency (BSH) for providing access to the research vessel Deneb. The authors are responsible for the contents of this publication.

References

[1] A. Amro *et al.*, "Navigation Data Anomaly Analysis and Detection," *Information*, vol. 13, no. 3, 2022.
[2] M. Balduzzi *et al.*, "A Security Evaluation of AIS Automated Identification System," in *In Proc. of ACSAC*, 2014.
[3] J. Bhatti and T. E. Humphreys, "Hostile Control of Ships Via False GPS Signals: Demonstration and Detection," *Journal of the Institute of Navigation*, vol. 64, no. 1, 2017.
[4] V. Bolbot *et al.*, "A novel cyber-risk assessment method for ship systems," *Safety Science*, vol. 131, 2020.
[5] M. Caprolu *et al.*, "Vessels Cybersecurity: Issues, Challenges, and the Road Ahead," *IEEE Commun. Mag.*, vol. 58, no. 6, 2020.
[6] J. Giraldo *et al.*, "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surv.*, vol. 51, no. 4, Jul. 2018.
[7] C. Hemminghaus *et al.*, "BRAT: A BRidge Attack Tool for Cyber Security Assessments of Maritime Systems," *TransNav*, vol. 15, no. 1, 2021.
[8] IEC 61162-450:2018, "Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection," International Electrotechnical Commission (IEC), 2018.
[9] IMO MSC.302(87), "Resolution MSC.302(87) Adoption of Performance Standards for Bridge Alert Management," May 2010.
[10] IMO MSC.428(98), "Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems," June 2017.
[11] International Transport Forum, *ITF Transport Outlook 2021*, 2021.
[12] ISO 9241-210:2019, "Ergonomics of Human-system Interaction: Part 210: Human-centred Design for Interactive Systems," Standard, 2019.
[13] 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. EDP Sciences, 2021.
[14] M. S. Lund *et al.*, "Integrity of integrated navigation systems," in *In Proc. of CNS*, 2018.
[15] ——, "An attack on an integrated navigation system," *Necesse*, vol. 3, no. 2, 2018.
[16] D. Mehta *et al.*, "The Big Hack Explained: Detection and Prevention of PCB Supply Chain Implants," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 16, no. 4, 2020.
[17] P. Meland *et al.*, "A Retrospective Analysis of Maritime Cyber Security Incidents," *TransNav*, vol. 15, no. 3, 2021.
[18] J. Nielsen, "Estimating the number of subjects needed for a thinking aloud test," *Int. J. of Human-Computer Studies*, vol. 41, no. 3, 1994.
[19] F. O. Olowononi *et al.*, "Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 1, 2020.
[20] J. Pavur *et al.*, "A Tale of Sea and Sky On the Security of Maritime VSAT Communications," in *In Proc. of SP*, 2020.
[21] M. Riveiro *et al.*, "Maritime anomaly detection: A review," *WIREs Data Mining and Knowledge Disc.*, vol. 8, no. 5, 2018.
[22] M. Roesch *et al.*, "Snort: Lightweight intrusion detection for networks." in *Lisa*, vol. 99, no. 1, 1999.
[23] Safety4Sea, "Maersk line: Surviving from a cyber attack," The Editorial Team, May 2018. [Online]. Available: https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/
[24] K. Tam and K. Jones, "Cyber-Risk Assessment for Autonomous Ships," in *In Proc. of Cyber Security*, 2018.
[25] The Zeek Project, "Zeek," 2021. [Online]. Available: https://zeek.org/
[26] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Comp. & Security*, vol. 72, 2018.
[27] D. I. Urbina *et al.*, "Limiting the impact of stealthy attacks on industrial control systems," in *Proc. of CCS*, 2016.
[28] J. Wang, "The Art of Intrusion Detection," in *Computer Network Security: Theory and Practice*, 2009.
[29] K. Wolsing *et al.*, "Network attacks against marine radar systems: A taxonomy, simulation environment, and dataset," in *Proc. of LCN*, 2022.