Guiding Ship Navigators through the Heavy Seas of Cyberattacks

Merlin von Rechenberg[•], Nina Rößler[○], Mari Schmidt[•], Florian Motz[○], Elmar Padilla[•], Jan Bauer[•]
[•]Cyber Analysis & Defense, [○]Human Systems Engineering
Fraunhofer FKIE, Wachtberg, Germany
{merlin.rechenberg, nina.roessler, mari.schmidt, florian.motz, elmar.padilla, jan.bauer}@fkie.fraunhofer.de

***Abstract*—In the maritime sector, which is increasingly exposed to threats from cyberspace, not only on-shore systems are prone to cyberattacks but also maritime systems onboard vessels have serious vulnerabilities and can therefore become easy targets. Nevertheless, in practice, there is still a lack of network-based Intrusion Detection Systems (NIDSs) for those systems to appropriately protect against possible attacks by providing alarms and instructions supporting bridge crews. For this reason, we present a *Cyber Incident Monitor (CIM)* as a security framework consisting of a NIDS and a nautical human machine interface (HMI). While the NIDS can detect several known attack vectors in maritime networks, the HMI provides tailored guidance for nautical operators to adequately respond in the event of a cyberattack.**

I. Introduction

With the growing digitalization of the commercial shipping industry also the surface for cyberattacks increases [2], targeting both, on-shore and off-shore maritime infrastructures. Reported incidents further confirm this increasing trend [8]. Whereas attacks against on-shore logistics infrastructures have been known to cause great economic damage in the past, recently, also various cyber threats on maritime systems onboard vessels have been demonstrated to be possible, including attacks on integrated bridge systems (IBSs) [6]. Such attacks not only have a strong economic impact, but can also threaten the safety of the environment and, more seriously, of crews and passengers. However, in practice, cybersecurity incidents stay largely undetected until they cause catastrophic events [9]. Attacks targeting the automatic identification system (AIS), global navigation satellite systems (GNSSs), and satellite-based communication are well understood and, nowadays, often do not require expert knowledge or expensive hardware equipment. Consequently, research on maritime cybersecurity is concerned with developing appropriate preventive and detective methods against such attacks. However, attacks that directly target IBSs at network-level, and particularly appropriate countermeasures, have only recently become the focus of current research. In this context, cyber threats are explicitly mentioned in the IEC 61162-460 standard for higher safety and security as well as improvements of communication integrity in maritime networks, but concrete security solutions besides common and rather generic measures are missing.

Although the goal is ideally complete prevention of cyber incidents, this is generally difficult to achieve in practice. Hence, defense-in-depth requires additional security measures like NIDSs. Well-established tools such as *snort* or *zeek* have the advantage to provide broad and accurate coverage for unencrypted traffic of common Internet protocols. Thus, they are widely used for network analysis and intrusion detection in modern intranets and on-shore IT infrastructures.

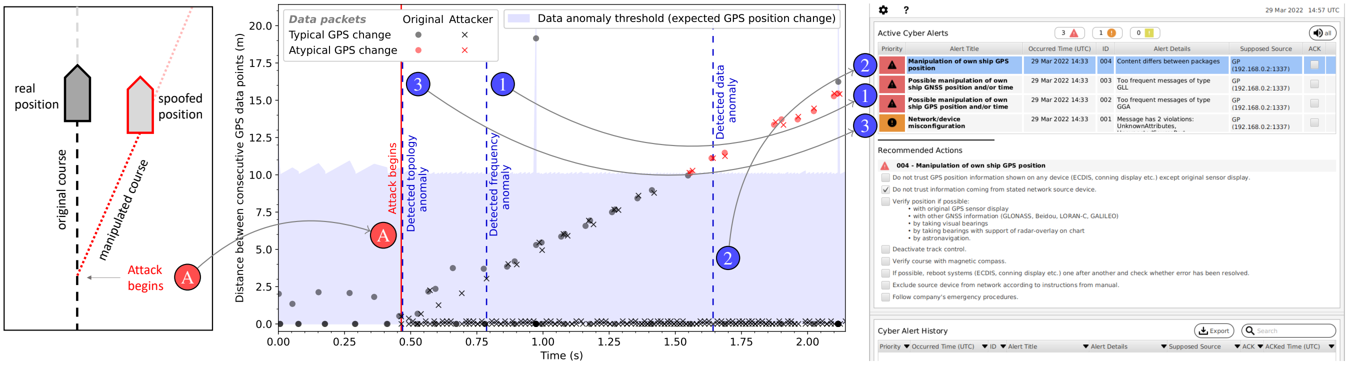
However, providing satisfying results for attacks against the special domain-specific protocols used in IBSs with conventional tools would require non-trivial configurations and adaptions. Therefore, we propose a novel NIDS framework specialized for the detection of attacks on ship navigation and tailored to the requirements of maritime systems, i.e., IBSs, which facilitates its deployment in general shipboard networks. At the same time, our approach provides an ergonomic HMI designed to enable nautical operators to quickly assess the extent of detected incidents and the resulting risks and initiate suitable response measures.[1]

II. Background & Related Work

In principle, there are two NIDS paradigms: i) misuse detection explicitly defining *abnormal* network behavior allowing for attack signatures, and ii) anomaly detection defining *normal* behavior. The latter has the potential to detect novel kinds of attacks or attacks that are difficult to define but may cause higher false positive rates, which sometimes hinders acceptance. Thus, reducing false positives poses a key challenge.

In maritime systems, both paradigms are promising to mitigate cyber threats, with anomaly-based methods currently predominating in the scientific community. In their extensive survey on state-of-the-art of maritime anomaly detection [7], Riveiro et al. conclude that there are already a few approaches for analyzing the network topology of maritime systems, but none represents an actual NIDS. In their recent work towards specialized NIDSs for maritime systems [1], Amro et al. propose multiple different anomaly detection methods for attacks on the communication of nautical data. To evaluate the performance of the detection, they use simulated attacks. Focusing on machine-in-the-middle (MitM) attacks, they conclude that those attacks can only be reliably detected by the proposed methods if adversaries are not using the full potential of the MitM position. However, the proposed NIDS constitutes an approach on the technical level but does not incorporate that future users are not security experts but rather nautical operators. To the best of our knowledge, there is no maritime NIDS that takes into account the unique needs of navigators who must assess incident alarms to determine the resulting risks and make time-critical decisions about how to respond.

[1] *CIM* was developed in the research project SINAV funded by the German Federal Ministry for Digital and Transport (BMDV).



29 Mar 2022 14:57 UTC

Active Cyber Alerts 3 ▲ 1 ● 0 !

Priority	Alert Title	Occurred Time (UTC)	ID	Alert Details	Supposed Source	ACK
▲	**Manipulation of own ship GPS position**	29 Mar 2022 14:33	004	Content differs between packages	GP (192.168.0.2:1337)	□
▲	**Possible manipulation of own ship GNSS position and/or time**	29 Mar 2022 14:33	003	Too frequent messages of type GLL	GP (192.168.0.2:1337)	□
▲	**Possible manipulation of own ship GPS position and/or time**	29 Mar 2022 14:33	002	Too frequent messages of type GGA	GP (192.168.0.2:1337)	□
●	**Network/device misconfiguration**	29 Mar 2022 14:33	001	Message has 2 violations: UnknownAttributes,	GP (192.168.0.2:1337)	□

Recommended Actions

▲ **004 - Manipulation of own ship GPS position**

□ Do not trust GPS position information shown on any device (ECDIS, conning display etc.) except original sensor display.
☑ Do not trust information coming from stated network source device.
□ Verify position if possible:
- with original GPS sensor display
- with other GNSS information (GLONASS, Beidou, LORAN-C, GALILEO)
- by taking visual bearings
- by taking bearings with support of radar-overlay on chart
- by astronavigation.

□ Deactivate track control.
□ Verify course with magnetic compass.
□ If possible, reboot systems (ECDIS, conning display etc.) one after another and check whether error has been resolved.
□ Exclude source device from network according to instructions from manual.
□ Follow company's emergency procedures.

Cyber Alert History

Priority ▼	Occurred Time (UTC) ▼	ID ▼	Alert Title ▼	Alert Details ▼	Supposed Source ▼	ACK ▼	ACKed Time (UTC) ▼

(a) Attack. (b) Detection. (c) Alerting & response.

Fig. 1. *CIM*'s capability 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 (c) that alerts and instructs bridge crews in case of cyber incidents.

III. Maritime NIDS for Ship Navigators

To bridge this gap, we introduce a *Cyber Incident Monitor (CIM)* for monitoring nautical communication. *CIM* is based on a maritime NIDS tailored for navigational IBSs and a specifically designed HMI. The detection focuses on on-the-side attacks within these systems since they are less complex to accomplish, more realistic, and thus more likely to occur than MitM attacks. On-the-side attacks can be executed by any maliciously introduced or compromised device in the network, whereas MitM attacks require the malicious device to be in a special network position, for the anomaly detection on the application layer, the NIDS utilizes three fundamental methods: ① protocol-based approaches identifying denial of service attacks and unusual frequency of message delivery, ② content-based approaches checking the plausibility of values and deviations between their payloads, and ③ structure-based approaches using a defined or learned topology to be expressed as a set of rules. Violations of such rules, e.g., induced by malicious devices, are detected. The detection methods of our approach have been simulatively evaluated using the *BRidge Attack Tool (BRAT)* [3]. The evaluation shows in general that the implemented attacks can be detected quickly and reliably by all three detection methods. Although the NIDS already includes approaches to reduce false positives, they cannot be eliminated completely with our approach, which consequently poses a challenge for future work.

To highlight the interaction of *CIM*'s NIDS and its HMI component, we briefly show a simulated course manipulation attack (Ⓐ in Fig. 1(a)). The adversary exemplarily attempts to change the displayed position of the vessel by superimposing forged position data. Even a stealthy, i.e., slow-growing, deviation from the original course induced by the attacker is detected promptly using *CIM*'s detection methods (Fig. 1(b)). Their individual indications can be weighted and combined to reduce false positives and, thus, further improve the effectiveness of our approach, before they are passed to the HMI.

CIM's ergonomic HMI, designed specifically for nautical operators, presents alarms and possible detections in a manner familiar to the user and in compliance with the IMO performance standards for bridge alert management [4]. Figure 1(c) shows the alerts issued by the system due to the exemplary course manipulation attack. Furthermore, *CIM* presents specific instructions as decision support for incident response in form of a checklist. Recommended actions include verifying potentially corrupted information, using alternate data sources to safely continue the journey, and taking steps to restore the bridge systems to a normal state. The HMI has been developed iteratively from defined user requirements and initial prototypes to the implemented application, following a human-centered design approach [5]. Four nautical experts participated in a formative evaluation. By observing, employing the think-aloud protocol, and conducting post-session interviews, we were able to elicit suggestions for improving the usability, which were incorporated in the final version of *CIM*. Similarly, the presented decision support has been defined and refined in several interviews with nautical experts.

Overall, with *CIM* we have developed a NIDS framework tailored to IBSs that can detect anomalies in the communication of nautical data and guide navigators through the heavy seas of cyberattacks by means of an ergonomic HMI.

References

[1] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation Data Anomaly Analysis and Detection," *Information*, vol. 13, no. 3, 2022.

[2] 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, pp. 90–96, 2020.

[3] C. Hemminghaus, J. Bauer, and E. Padilla, "BRAT: A BRidge Attack Tool for Cyber Security Assessments of Maritime Systems," *TransNav*, vol. 15, no. 1, 2021.

[4] IMO MSC.302(87), "Resolution MSC.302(87) Adoption of Performance Standards for Bridge Alert Management," May 2010.

[5] ISO 9241-210:2019, "Ergonomics of Human-system Interaction: Part 210: Human-centred Design for Interactive Systems," Standard, 2019.

[6] M. S. Lund, J. E. Gulland, O. S. Hareide, Ø. Jøsok, and K. O. C. Weum, "Integrity of integrated navigation systems," in *In Proc. of the Conf. on Comm. and Network Security (CNS)*, Beijing, China, 2018, pp. 1–5.

[7] M. Riveiro, G. Pallotta, and M. Vespe, "Maritime anomaly detection: A review," *WIREs Data Mining and Knowledge Disc.*, vol. 8, no. 5, 2018.

[8] M. Schwarz, M. Marx, and H. Federrath, "A structured analysis of information security incidents in the maritime sector," 2021, arXiv 2112.06545.

[9] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & Security*, vol. 72, 2018.